U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

June 8, 2016

MS. ALEXA O'BRIEN
MUCKROCK NEWS
DEPT MR 17650
POST OFFICE BOX 55819
BOSTON, MA 02205-5819

FOIPA Request No.: 1329073-000
Subject: Carnivore

Dear Ms. O'Brien:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act. Enclosed is one CD containing 605 pages of previously processed documents and a copy of the Explanation of Exemptions. Please be advised, these are the only copies of these documents located in our possession. The original copies of these documents could not be located for reprocessing.

Additional records potentially responsive to your subject exist. The Federal Bureau of Investigation (FBI) has located approximately 1,594 pages total of records potentially responsive to the subject of your request. By DOJ regulation, the FBI notifies requesters when anticipated fees exceed $25.00.

If all potentially responsive pages are released on CD, you will owe $40.00 in duplication fees (3 CDs at $15.00 each, less $5.00 credit for the first CD). Releases are made on CD unless otherwise requested. Each CD contains approximately 500 reviewed pages per release. The 500 page estimate is based on our business practice of processing complex cases in segments.

Should you request that the release be made in paper, you will owe $79.70 based on a duplication fee of five cents per page. See 28 CFR §16.10 and 16.49.

If you agree to receive all responsive material on CD, you will receive a $5.00 credit towards your first interim CD. As a result, we must notify you there will be a $25.00 charge when the second interim release is made in this case. At that time you will be billed for the $10.00 remaining from the $15.00 free of the first release, as well as the $15.00 duplication fee for the second release, for a total of $25.00.

Please remember this is only an estimate, and some of the information may be withheld in full pursuant to FOIA/Privacy Act Exemptions(s). Also, some information may not be responsive to your subject. Thus, the actual charges could be less.

Requester Response

No payment is required at this time. If your request does not qualify for eFOIA releases, you must notify us in writing within thirty (30) days from the date of this letter of your format decision (paper or CD). You must also indicate your preference in the handling of your request in reference to the estimated duplication fees from the following four (4) options:

☐ I am willing to pay estimated duplication/ international shipping fees up to the amount specified in this letter.

☐ I am willing to pay fees of a different amount.

Please specify amount: _____

☐ Provide me 100 pages or the cost equivalent ($5.00) free of charge. If applicable, I am willing to pay International shipping fees.

☐ Cancel my request.

If we do not receive your duplication format decision and/or estimated duplication fee selection within thirty (30) days of the date of this notification, your request will be closed. Include the FOIPA Request Number listed above in any communication regarding this matter.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You have the opportunity to reduce the scope of your request; this will accelerate the process and could potentially place your request in a quicker processing queue. This may also reduce search and duplication costs and allow for a more timely receipt of your information. The FBI uses a multi-queue processing system to fairly assign and process new requests. Simple request queue cases (50 pages or less) usually require the least time to process.

Please advise in writing if you would like to discuss reducing the scope of your request and your willingness to pay the estimated search and duplication costs indicated above. Provide a telephone number, if one is available, where you can be reached between 8:00 a.m. and 5:00 p.m., Eastern Standard Time. Mail your response to: **Work Process Unit; Record Information/Dissemination Section; Records Management Division; Federal Bureau of Investigation; 170 Marcel Drive; Winchester, VA 22602**. You may also fax your response to: 540-868-4997, Attention: Work Process Unit.

For questions regarding our determinations, visit the www.fbi.gov/foia website under “Contact Us.” The FOIPA Request number listed above has been assigned to your request. Please use this number in all correspondence concerning your request. Your patience is appreciated.

Want to send this story to another AOL member? Click on the heart at the top of this window.

Reno describes FBI Internet-wiretap system review

WASHINGTON, July 27 (Reuters) - U.S. Attorney General Janet Reno described on Thursday a two-step process to review a new FBI Internet-wiretap system called Carnivore that has raised privacy concerns.

With lawmakers and privacy advocates concerned the system allows for widespread surveillance of e-mails, Reno said the first step will be for a group of academic experts to conduct a detailed review of the computer program's source code.

"Those experts will report their findings to a panel of interested parties, people from the telecommunications and computer industries, as well as privacy experts," Reno told her weekly Justice Department news briefing.

"I'm very anxious to get this review under way. The FBI is working on it, and representatives of the bureau are meeting with privacy advocates and representatives of the telecommunications and computer industry to pursue it and to develop a protocol for the review," she said.

The system allows the FBI to intercept the e-mails of a criminal suspect among the flood of other data passing through an Internet service provider.

FBI officials maintain the court-authorised wiretaps will only focus on criminal suspects who are targets of an investigation. But privacy advocates fear the system may cast too wide a net, encompassing private information about legal activities.

Reno said the two-step process was worked out with the FBI, and that she wanted the review to be done "as soon as possible."

She said the system would not be suspended until the review has been completed. "I think that we will continue to make sure that it is implemented carefully and there is no abuse in its use."

In a letter to Reno, 27 House of Representatives Republicans and one Democrat expressed "strong reservations" about the system and urged Reno to halt its operation "until the serious privacy issues have been satisfactorily answered."

The lawmakers added, "People should feel secure that the federal government is not reading their e-mail, no matter how worthy the objective."

Reno stopped short of agreeing to release the source code. The American Civil Liberties Union has asked for it to be made public so it could evaluate the software's true capabilities.

14:06 07-27-00

Want to send this story to another AOL member? Click on the heart at the top of this window.

Bill Addresses E-mail Surveillance

By D. IAN HOPPER
.c The Associated Press

WASHINGTON (AP) - A move is under way in Congress to increase the burden on federal law enforcement agencies to justify monitoring people's e-mail messages and other communications.

Rep. Bob Barr confirmed that he and his staff are at work on a bill that would rein in the FBI's new ``Carnivore'' surveillance system and place additional restrictions on telephone wiretaps as well.

Barr, R-Ga., said he was concerned about computer eavesdropping capability before attending a hearing on Capitol Hill earlier this week, and he said he ``came out of it scared.''

Privacy advocates and computer experts called Carnivore a ``black box'' in testimony Monday, and said only the FBI knows what it truly does. They also contended that information the FBI gets from the device, installed at a suspect's Internet service provider, is far more than what could be gleaned from a telephone wiretap and statutes governing telephone surveillance are being misused.

In a telephone ``trap-and-trace'' or ``pen register'' wiretap, authorities can get a list of phone calls made to and from a certain telephone number. The usable information is limited to the 10-digit telephone numbers and the time of the call, and the phone company, when given a court order, provides the information.

Current laws and judicial precedent say that the numbers a person dials are not private communications, and therefore authorities do not need to show that a crime has been committed.

With Carnivore, that statute is being extended to the Internet world.

The details of Barr's bill aren't clear yet, but he said it would address the issue of translating telephone wiretap law to the Internet by designing strict constraints for monitoring the medium. It would also make sure that evidence gained from an e-mail tap would not yield more information than a similar court order for a telephone tap.

The FBI's new surveillance mechanism sits at the subject's ISP and scans the addressing information coming from or going to the suspect's computer. This can reveal far more information than a simple e-mail address, such as a subject line describing the contents of the message.

``Capturing Internet origin and destination address instead of 'numbers dialed' could create a much more intrusive form of surveillance that is not clearly supported by law,'' said Alan B. Davidson, staff counsel at the Center for Democracy and Technology.

For authorities to be able to request e-mail contents they must show probable cause and obtain a search warrant. The same is true for listening in on a telephone call.

Regarding the inner workings of Carnivore, the FBI is resisting a Freedom of Information Act request by the American Civil Liberties Union for Carnivore's computer code, but said it will submit to an external review.

Since the Carnivore computer, devoid of keyboard and mouse, sits at the suspect's ISP and is locked down from any manipulation from non-FBI personnel, Internet providers have bristled at the idea of letting it sit on their networks.

Donald M. Kerr, assistant director of the bureau's laboratory division, said in an interview that the FBI would love to have the ISP provide the information authorities need, but the cost and technical knowledge can be prohibitive for small Internet companies.

Peter William Sachs, a lawyer and president of ICONN, a small Internet provider in Connecticut, said the job could be done with two lines of computer code, and called it a ``trivial'' task.

Barr concurred, saying "I'm not satisfied with the FBI's explanation."

But he will have a stiff challenge in keeping apace of the changes in technology.

Not only can Carnivore monitor e-mails, Kerr said, but it also can monitor Web browsing, chat rooms and all sorts of other communications.

However, it is the FBI's argument that although Carnivore can read those things, it's a difference between "capability and authorization," Kerr said.

"People seem to conjure up this vision that FBI personnel are unsupervised and unconstrained in the use of these tools," he said. "To misuse these authorities and to go outside the scope of the court order is to commit a federal felony. It's, to me, not conceivable that groups of our employees would run that kind of risk in doing their job."

Kerr again noted a separate audit trail maintained by Carnivore that keeps track of its activity and configuration, and said that trail is an extra safeguard against misuse.

Barr said he expects resistance from other legislators, even from other Republicans, but said he will not let the FBI go unchecked.

"They want to just go out and rely on scaring people to death, that if they don't get this authority, the terrorists will take over the country, and say 'we're out to save the world,' " Barr said.

AP-NY-07-27-00 0904EDT

7/27/00


YES. WE SPY ON YOUR E-MAIL, BUT IT'S FOR YOUR OWN SAFETY. YOU CAN TRUST US WITH YOUR PERSONAL INFORMATION.
FBI
BY THE WAY... ...YOUR SON IS GAY, YOUR DAUGHTER'S PREGNANT AND YOUR AUNT IDA'S SHINGLES ARE FLARING UP AGAIN!
FBI
NEG
THE FREE LANCE-STAR

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of Doc. #24, OGC FRONT OFFICE FILE (PG. 151)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #37 (Page 555)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

__1__ Pages were not considered for release as they are duplicative of DOC. #26, OGC FRONT OFFICE FILE (PG. 153)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #38 (Page 556)

XXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Representing Florida's 12th District
Charles T. Canady
Chairman, House Judiciary Subcommittee on the Constitution
2432 Rayburn House Office Building • Washington, D.C. 20515 • 202-225-1252

For Immediate Release
July 27, 2000

Contact: Michelle Morgan Knott
(202) 225-1252

Rep. Canady Introduces Bill to Update Wiretap Laws

E-Mails and Stored Internet Communications Would Be Covered

WASHINGTON, D.C. — **Rep. Charles T. Canady** (R-FL), Chairman of the House Judiciary Subcommittee on the Constitution, today introduced the Electronic Communications Privacy Act of 2000. The bill would update the federal wiretap laws to cover e-mail and stored electronic communications, as well as provide special requirements for government tracing of e-mail addresses. Canady is joined by original cosponsor Rep. Asa Hutchinson (R-AR).

> **"This legislation helps move our federal wiretap laws into the 21st Century," Canady said. "We have entered a new age with the Internet, and we need a new law to reflect the rapid changes in technology. While this legislation does not answer all the difficult issues raised by recent technological advances, it does provide for some reasonable reforms that will protect the privacy rights of Americans."**

Earlier this week, Rep. Canady chaired a Constitution Subcommittee hearing on Fourth Amendment issues raised by the FBI's "Carnivore" program. The FBI designed and developed Carnivore to isolate, intercept and collect communications that are the subject of lawful court orders. The July 24th hearing featured witnesses from law enforcement, civil liberty organizations, privacy organizations and representatives from the business community.

BILL SUMMARY

The Electronic Communications Privacy Act of 2000 has three sections. The first section amends the "statutory exclusionary rule" to also exclude from use as evidence illegally intercepted "electronic communications" and illegally obtained "stored electronic communications." The bill simply adds electronic communications to the previously covered wire and oral communications.

The second section of the bill requires the federal government to produce annual reports regarding its requests for orders for the disclosure of "stored electronic communications." This reflects virtually identical disclosure requirements the federal government must meet regarding the use of electronic wiretaps.

The final section of the legislation amends the definition of "pen register" and "trap and trace" devices, defining them to allow the identification of an "e-mail address." In addition, the section requires that, if a pen register or trap and trace device is used to identify an e-mail address, the

-more-

federal government must first demonstrate to a court that "specific and articulable facts reasonably indicate that a crime has been, is being, or will be committed, and information likely to be obtained by such installation and use [of a pen register or trap and trace device] is relevant to an investigation of that crime."

For a copy of Rep. Canady's legislation (7 pages) please call Michelle Knott at (202) 225-1252.

###

OMAHA DAILY HERALD FOUNDED [illegible]
OMAHA DAILY WORLD FOUNDED BY GILBERT M. HITCHCOCK 1885
OMAHA WORLD-HERALD FIRST PUBLISHED JULY 10, 1889

Omaha World-Herald

JOHN GOTTSCHALK, *Publisher*
LAWRENCE D. KING, *Executive Editor* FRANCIS L. PARTSCH, *Editorial Pages Editor*
DEANNA J. SANDS, *Managing Editor*

Is Carnivore on a Leash?

The FBI insists that its recently disclosed "Carnivore" Internet surveillance system is not a wide-spectrum threat to privacy. Federal operatives say that in fact it is used only pursuant to normal Justice Department procedures. In many or most instances these rest on a judge-signed surveillance order keyed to evidence that a serious crime is being or has been committed.

These are welcome assurances. But for the moment, that's all they are. As one conservative Alabama congressman said in a Monday subcommittee hearing, "What you're saying is, 'Trust us.'"

That's the nub of the problem. The ominously named Carnivore is so encompassing, so sophisticated, so tweakable — and its inner workings so closely guarded — that it's almost impossible for anyone besides its operators to know what it's really examining and really ignoring.

This differs markedly from telephone wiretapping. In classic wiretapping, if a tap is to be placed on one phone, agents have traditionally opened a junction box and attached connectors to terminals for that phone and that phone only. In some instances, only incoming and outgoing phone numbers are registered. In others, depending on what a judge thinks is necessary, actual conversations are recorded.

In a sense, comparable service can still be delivered to law enforcement agencies by a customer's Internet service provider. It is reasonably assured that only one client's communications will be looked at.

Carnivore is different. If the service provider allows it to be installed, the Carnivore filter is placed directly in the path of the company's entire Internet data flow. The filter is supposed to "sniff" only what it is set to — for example, incoming and outgoing e-mail addresses for just one account. Or it can probe more deeply. But everything moves through it — from child porn and drug deals to recipes shared with Aunt Nell or strategy discussions between politicians and their policy advisers.

The most comforting observation we've heard so far came from the FBI's Marcus Thomas, a developer of the system. He told The Wall Street Journal that if Carnivore actually were told to read everything that came through, it would bog Internet traffic down to a degree that couldn't go unnoticed. That sounds plausible, a little like trying to force a firehose's output through a soda straw.

Still, the temptation to look at more than what is authorized, whether with good intentions or evil, is powerful. Law enforcement has done it repeatedly in the past, undercutting to some extent the assurances that it won't happen with Carnivore. And the immense power that Carnivore possesses only enhances the pressure to use it.

That's why factions as divergent as extremely liberal and deeply conservative members of Congress, along with the ACLU and many just plain citizens, are nervous about the device. Its technical ability to run afoul of the Fourth Amendment's protections against unreasonable searches is unmistakable.

What this flap points to above all else is that communication technology has far outpaced the nation's wiretap laws, some of which date back to the early 20th century. This is a problem only Congress can address. To its credit and that of the administration, some attempts are in progress.

The administration has asked that federal laws on Internet communications security be upgraded to assure that they match the kind of judicial and administrative restraint that already applies to phone taps. Sen. Patrick Leahy, D-Vt., has written a broad-based Internet privacy bill, and Sen. Orrin Hatch, R-Utah, has introduced another, somewhat narrower measure.

Such attempts, while laudable, will not be reconciled for months, perhaps years. Meanwhile, the FBI has offered to let an independent third party review whether Carnivore's deeds match the agency's words. That would be welcome, but Carnivore ought to be shut down until such a review can be completed and reports issued to Congress.

No modern law enforcement agency should be entirely deprived of surveillance techniques, but putting Carnivore on hold wouldn't do that. It would, on the other hand, provide at least some assurance to innocent parties that their private lives aren't open books. That could hardly be a bad thing.

USA TODAY

DATE: 7-28-00

PAGE: 1

Warrants for online data soar

Demands served on Internet, e-mail providers up 800%, study finds

By Will Rodger, USATODAY.com

The number of search warrants seeking citizens' online data has soared more than 800% during the past few years, a USA TODAY study shows.

The findings, based on an examination of warrants served on the top Net service provider, America Online, surprised federal lawmakers and civil libertarians and prompted calls for legal reforms.

Searches for the online data typically involve cases ranging from harassment and child pornography to violent crime and fraud and are aimed at discovering the identity and tracking the activities of subscribers. Last year, AOL was served with 301 search warrants, up from 33 in 1997. This year, state and local investigators have served 191 warrants through July 17, filings show. AOL had no comment.

All Internet service providers and Web mail providers in the USA "have experienced a significant increase in the number of search warrants and subpoenas," said Andrew Grosso, an attorney who specializes in computer law.

Congressional leaders informed of the findings said they will examine legal standards applied to such Internet investigations. At a minimum, House Majority Leader Dick Armey, R-Texas, said, police need to tell Congress when, why and how they perform electronic searches. The White House already has pledged to move soon to protect electronic data.

Critics and privacy experts fear that electronic surveillance of all types, if not tightly controlled, can violate laws against unreasonable police searches. The FBI's Thomas Gregory Motta says there is little reason for concern.

So far, he says, the law has treated stored records, such as e-mail, as it treats other documents, such as letters and diaries, which can be seized from a home with a simple search warrant. Often, though, authorities ask for more than e-mail.

A random sample of 14 such warrants in the past 18 months showed that 10 asked for all data the service had on targeted subscribers. "They can get a record of what times you dialed in, where you dialed in from, how long you were online, what activities you were engaged in, what Web sites you visited, what chat sessions you were in and what you said there," said Mark Rasch, a former federal prosecutor and vice president for cyber law at Global Integrity in suburban Washington.

10

Doc 41

July 28, 2000

BARR BILL UPDATES WIRETAP LAWS
MEASURE ENHANCES ELECTRONIC PRIVACY PROTECTION

WASHINGTON, D.C. -- U.S. Representative Bob Barr (GA-7) announced today he was introducing the "Digital Privacy Act of 2000." The legislation updates wiretapping laws to enhance privacy protections and bring them in line with technological developments, such as the Internet, wireless phones, and electronic mail. Specifically, the measure would:

- Extend reporting statues requiring law enforcement to report on its interception of electronic communications, in addition to the telephone wiretap reports already required.
- Block the use of electronic evidence in court if it is obtained illegally.
- Stop unchecked government access to the identities of computer users unless there is reasonable evidence a crime has been committed.
- Stop the government from tracking the location of cell phone users without a court order.

"As the White House recently acknowledged, our wiretapping laws have fallen far behind the technological explosion of the past decade. For example, under current law, e-mails receive less legal protection than both traditional postal mail and telephone conversations," said Barr.

"The Digital Privacy Act corrects some of the most glaring contradictions and loopholes in current law. As systems from NSA's Project Echelon to FBI's Carnivore have proven, technological advances make large scale surveillance easier than ever before. It is vital we safeguard our civil liberties by making certain the law changes to prevent longstanding Fourth Amendment protections from being eroded," Barr continued.

Barr, a Member of the House Judiciary Committee, has served with both the Department of Justice and the Central Intelligence Agency.

--30--

To send a letter to the editor on this topic

To have a regular e-mail update delivered t you.

BACK TO PRESS RELEASES

http://www.house.gov/barr/p_072800.html

Doc #4
8/2/00

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

18 Page(s) withheld for the following reason(s): SEALED COURT DOCUMENT FROM USDC CENT DIST. OF CAL. NO. CR99-285(A)-ABC

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #1 (Pages 562 - 579)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

EARTHLINK

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA - WESTERN DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INSTALLATION OF A PEN REGISTER AND TRAP AND TRACE DEVICE,	Criminal No. 99-2713M ORDER: (1) DENYING MOTION TO QUASH ORDER AUTHORIZING PEN REGISTER; AND (2) GRANTING APPLICATION TO EXTEND ORDER AUTHORIZING PEN REGISTER

This case raises the question whether this court has the legal authority under the pen register statute, 18 U.S.C. § 3122, et seq., to issue an order requiring an Internet service provider (ISP) to install a device which captures the time, date, source and destination addressing information of electronic mail (e-mail) messages sent to and from an e-mail address maintained by a customer at the ISP. After consideration, the court finds that it has the legal authority under the pen register statute to issue such an order.

The discussion of this issue arises in the context of an ongoing criminal investigation. The court does not want to compromise the integrity of that criminal investigation. Accordingly, the description of the facts out of which the current dispute arises deliberately omits factual information which could alert the subject

Doc. #2

or subjects of the investigation to the existence of and the techniques used in the investigation.

On December 2, 1999, the government, through an Assistant United States Attorney, presented to the court an ex parte application for the issuance of an order in the nature of a pen register. The application contained information that a federal criminal investigatory agency was seeking to locate a federal fugitive, that agents of the federal agency believed that the fugitive was maintaining contact with a specific named close friend or relative ("the subject") by means of e-mail transmissions sent to the subject, and that the subject maintained an Internet service account with a designated Internet service provider ("ISP") under the subject's name. This court issued an order providing that the government agency "may install a pen register and trap and trace device to register time, date, and source and destination addressing information of the electronic mail messages sent to and from the subject Internet account, including information regarding the true source of the messages without geographic limitation."

The government agency served the order on the ISP. The ISP and the government had some initial discussion regarding the order. Eventually, the ISP attempted to comply with the order by providing the agency with the "headers" (minus the subject or regarding line) of numerous incoming messages to the subject's e-mail account and the "headers" of a few outgoing messages (with the subject or regarding information deleted) from the subject account. The government is not satisfied with this response, contending that the terms of the order entitle it to install its own device on the premises of the ISP connected to ISP's equipment.

As a result of this dispute, the ISP has now moved to quash or modify the order. The government has opposed the motion to quash and separately submitted an ex parte application requesting an extension of the court's previous order.

At an initial scheduling conference, the parties represented that the court's original Order, issued December 2, 1999, would expire February 4, 2000. This court scheduled a hearing on the ISP's motion to quash or modify the order on February 4, 2000. It now appears to the court that the order has already expired. The statute provides that the court may issue an order authorizing the installation of a pen register "for a period not to exceed 60 days." 18 U.S.C. § 3123(c)(1). The Order was issued on December 2, 1999. Pursuant to the terms of the statute, the Order expired 60 days thereafter on January 31, 2000.

There is no presently effective order in place which this court may quash. The court therefore denies the ISP's motion to quash as moot.

Although that ruling resolves the pending motion of the ISP to quash, it does not resolve the underlying issue whether the court has the authority to issue an order. That issue is now presented to the court because the court must decide the government's application to extend the order.

The statute provides that:

> "the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified

to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."

18 U.S.C. § 3123(a).

The government has certified to the court that the information likely to be obtained by the pen register or trap and trace device is relevant to an ongoing criminal investigation. This court accordingly has authority to issue a proper pen register or trap and trace order. The question presented here is whether the device which the government seeks to install is a device described and authorized in the statute.

The statute defines a "pen register" as:

"a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached . . . ."

18 U.S.C. § 3127(3).

The statute describes a "trap and trace device" as:

"a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted."

18 U.S.C. § 3127(4).

It is apparent that a pen register, as defined in the statute, is intended to be a device which captures the telephone numbers dialed by a target phone. A trap and trace device is intended to capture the telephone numbers of telephones which make calls to a target phone. It is also fairly clear that the drafters of the pen

register statute did not contemplate that the statute would be used to authorize the issuance of court orders to capture the e-mail addresses of persons sending e-mail to and receiving e-mail from a targeted e-mail address.

The statutory definition of a pen register describes a device attached to a telephone line. 28 U.S.C. § 3127(3). The statutory definition of a "trap and trace device" does not limit the description to a device attached to a telephone line. 28 U.S.C. § 3127(4). "Nonetheless, it appears from the construction of related sections of the statutes governing trap and trace devices that they include only devices that are attached to a telephone line." In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F.Supp. 197, 200 (C.D. Cal. 1995) (hereafter "In re Cellular Digital Analyzer"). An order for use of both pen register and trap and trace devices must include "the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached . . . ." 18 U.S.C. § 3123(b)(1)(C).

It is clear that the government here does not intend to attach either a conventional pen register or a trap and trace device to the subject's telephone line. The government's opposition to the ISP's motion to quash contains a description by a technician declarant of how the government intends to implement the requested order. The government would install a computer program called "Carnivore" on the ISP's network, probably on a "router" used by the ISP. A "router" is described as a transmission device that processes packetized network information. Both the router and the ISP's network are connected to the telephone lines and transmit packetized network information over

telephone lines. The Carnivore software program would look for the target's log-in name (presumably for outgoing e-mail) or the target's electronic mail name (presumably for incoming e-mail). The program would then capture the "header" information associated with the e-mail message, including the time, date, and addressing information, including Internet identity, for messages sent to or from the target account. The program would not capture the subject or regarding line of the e-mail message or the content of the message. The captured material would be stored on a government computer which presumably would be attached to the ISP's router.

A conventional pen register is attached to telephone lines and captures the telephone number dialed by the target telephone. A trap and trace device is attached to telephone lines and captures the telephone numbers calling the subject telephone. Here, the government's requested device is a computer and software program attached to the ISP's equipment which is, in turn, connected to telephone lines and which captures the Internet e-mail addresses of persons sending to or receiving e-mail from the target. There appears to be no significant difference between capturing telephone numbers with a pen register or trap and trace device and capturing e-mail addresses with the government's proposed computer and software program.

This court acknowledges that the pen register statute, 18 U.S.C. § 3122, et seq. is contained in Title III of the Federal Electronic Communications Privacy Act of 1986, that one of the evident purposes of that statute is to regulate government intrusion into private communications, and that the statute should be strictly construed. In re Cellular Digital Analyzer, 885 F.Supp. at 200. This

court finds that the intrusion into otherwise private activity which would be allowed by the issuance of the government's requested order is no greater than the intrusion created by the issuance of a conventional pen register order. Although apparently not contemplated by the drafters of the original statute, the use of a pen register order in the present situation is compatible with the terms of the statute. Accordingly, the court will grant the government's application for the continued use of a pen register and issue an appropriate order.

For the reasons stated above, the ISP's motion to quash the original order authorizing the installation of a pen register is denied as moot. The government's application for the continued use of a pen register is granted.

IT IS SO ORDERED.

DATED: February 4, 2000

JAMES W. McMAHON
United States Magistrate Judge

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

4 Page(s) withheld for the following reason(s): SEALED COURT DOCUMENT FROM USDC CENT DISTRICT OF CALIFORNIA NO. 00-0249M

X The following number is to be used for reference regarding these pages: DOCUMENT #3 (Pages 587-590)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

UNITED STATES MARSHALS SERVICE
Investigative Services Division
Electronic Surveillance Unit

Office: (703) 285-3200, Facsimile: (703) 285-3215

b6-1
b6-3
b7c-1
b7c-3

TO: [redacted]

FROM: [redacted]

DATE: 02/02

NUMBER OF PAGES: 18 EXCLUDING COVER SHEET

COMMENTS:

WARNING: MANY FACSIMILE MACHINES PRODUCE COPIES ON THERMAL PAPER. THE IMAGE PRODUCED IS HIGHLY UNSTABLE AND WILL DETERIORATE SIGNIFICANTLY IN A FEW YEARS. IT SHOULD BE COPIED ON A PLAIN PAPER COPIER PRIOR TO FILING AS A RECORD.

Doc. #4

UNITED STATES MARSHALS SERVICE

Office of the Assistant Director for Investigative Services
600 Army Navy Drive
Suite 1200 - Crystal Square 4
Arlington, VA 22202
Phone: (202) 307-9110
FAX: (202) 307-9299 or (202) 307-9337

To: Marcus Thomas	Fax #:
From: [redacted]	
Date: 02/07	
Number of Pages: (excluding cover sheet) 5	
MESSAGE: Call me with any questions [redacted] Thanks	

b6-3
b7C-3

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

7 Pages were not considered for release as they are duplicative of DOCUMENT #2 OF THIS FILE

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #4, PGS. 3-9 (Pages 593 - 599)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

DECLARATION

I Edward Hill hereby declare as follows:

1. I am a Special Agent with the Federal Bureau of Investigation, and have been an Agent for 10 years. I specialize in technical equipment, including electronic surveillance equipment. I am familiar with the Internet and with surveillance devices used for the Internet.

2. If authorized by this court, I or other technicians intend to install a program called Carnivore to obtain the information sought in this order. The program will be installed on EarthLink's network, most likely on a "router" used by EarthLink. A "router" is a transmission device that processes packetized network information. Both the router and EarthLink's network are connected to the telephone lines and transmit packetized network information over the telephone lines. The Carnivore software program watches the incoming telephone traffic to EarthLink and looks for the targeted subscriber's log-in name or electronic mail account name. If it finds the target's log-in name, the program follows the target while the target is on line. The program then captures only the header information for electronic mail messages sent or received by the target while the target is on line. If the program finds the target's electronic mail account name, it will capture the header information associated with that electronic mail message. Specifically, the program will capture the time, date, and the addressing information (i.e., Internet identity) for electronic mail messages sent to or from the account. The program will not

capture the subject or regarding line on the electronic mail message, nor does it capture the content of the message or any information concerning the target's other on line activity.

3. Although the program is capable of capturing more than the information authorized under the order, I or the installing technicians will configure the program in a manner that will prevent the program from capturing any information that is not authorized under the order. In addition, the computer used to run the program has limited memory capacity and limited ability to process information. Because of these limitations the computer used to run the program would be overloaded within a few minutes if it attempted to collect all of the information on EarthLink's 8 to 10 million e-mail messages. Moreover, the program will be installed on a particular entry point into EarthLink's network, and as such would not have access to all of EarthLink's customers.

4. The program should not create a security risk for EarthLink. Although the Carnivore program is remotely accessible, it has several security provisions that prevent an intruder from obtaining unauthorized access to EarthLink's system. Even if an intruder did obtain such access, the program lacks a TCP/IP protocol stack, which means that the intruder would be unable to communicate with EarthLink's system from the government's computer. I and other agents with whom I work have installed this program at many other service providers (including AT&T) and have not had security problems or objections from the providers.

6C-1
67C-1

From: [redacted]
To: BOWMAN, SPIKE (MARION) [redacted]
Date: 4/5/00 5:29PM
Subject: [redacted]

I just received a call from [redacted] at OIPR. To state that she is unhappy with iTOS and the UBL Unit would be an understatement of incredible proportions. I will try to relate what [redacted] thinks has happened with the above named FISA.

[redacted] secured an ELSUR FISA very quickly on [redacted] at the request of [redacted] states that she was assured that the FBI had special software which could do what the FBI said it could do. In fact [redacted] states that the technical people in Quantico approved the FISA language.

The FBI technical people went to install the FBI software a[redacted] to accomplish the electronic surveillance on March 16.

The software was turned on and did not work correctly. The FBI software not only picked up the E-Mails under the electronic surveillance of the FBI's target, [redacted] but also picked up E-Mails on non-covered targets. The FBI technical person was apparently so upset that he destroyed all the E-Mail take, including the take on [redacted] is under the impression that no one from the FB[redacted] was present to supervise the FBI technical person at the time. Now the FBI technical people want to run a new software experiment at the carrier to see if it works.

62-2
6C-1
6C-3
67C-1
67C-3

[redacted] states that OIPR was never told that the FBI software was experimental. OIPR was informed that it would work. The FBI technical people are still trying to make it work in [redacted], and want to resume the electronic surveillance. The FBI people in [redacted] also want a physical search warrant to pick up the E-Mails from the carrier, which the FBI picked up on the target, but destroyed.

[redacted] informed me that the FBI does not have the authority to resume electronic surveillance until she receives a written explanation of what has happened and she files something with the court. Obviously, she has no intention of securing a search warrant either until this is straightened out.

When you add this story to the FISA mistakes covered in the E.C. I have prepared to go to the field, and which is in NSLU for signature before it goes to [redacted] for his signature, you have a pattern of occurrences which indicate to OIPR an inability on the part of the FBI to manage its FISAs.

[redacted] and [redacted] please see me ASAP.

Thanks
[redacted]

CC: [redacted]

DOC. #5

From: [redacted]
To:
Date: Tue, Apr 11, 2000 9:00 AM
Subject: DITU Legal Issues

[redacted]

The attached sets out a few issues we would like to discuss with you so that we can work toward providing a reasonalbe and practical guideline to personnel in our Unit and the Field.

My number is 703[redacted] I will be on leave from Thursday through next Tuesday.

CC: [redacted] MARCUS C THOMAS;

b6-1
b7C-1

Doc. #6

[redacted] 6C-1 67C-1

The following sets out some of the legal issues facing DITU as well as some thoughts on ways to proceed. We need your legal guidance in this matter to formulate a reasonable and prudent course of action, as well as a practical working guide for the personnel of DITU and the Field Office personnel involved in Data Intercepts. I am sure there are other issues and ideas, but this may be a good start. Call me to discuss this in more detail. I am willing to travel to your office at FBIHQ or to meet with you here at QT. If you need any clarification of technical concepts etc. you may call SSA [redacted] at 703-[redacted] or SSA [redacted] at 703 [redacted] 6C-1 67C-1

To initiate an intercept on a network or at an ISP, the DITU installs a collection device with appropriate filters set to capture data within the scope of the Court Order or the effective consent of a consenting party. This filtering process, a component of Etherpeek and Carnivore, filters based on TCP/IP standards. On occasion we encounter non-standard implementation of transmission control and Internet protocols within a network or at an ISP. Encountering non-standard implementation has led to inadvertently capturing and processing data outside the Order or Consent.

Issue I

In instances where we encounter non-standard implementation of a protocol which leads to the improper capture of data, two main concerns arise. The first, and of most immediate concern, is the formulation of a guideline to be followed in resolving the matter. This guideline should extend from the DITU personnel who installed and likely discovered the error, through DITU Management representatives, Field Division Case Agents, CDCs, notifications to AUSAs, Motions to Seal. etc.

Issue II

The second issue, critical in efforts to intercept the data under the Court's Order or under consent from a test account, is how FBI technical personnel, such as, Engineers, Computer Programmers and others, may lawful examine the collected data for the sole purpose of determining why the filters failed and what software changes need to be made to bring the collection in line with the scope of the existing Order. We need to look at the data to figure out what is wrong and how to fix it!!!

Issue III

A third issue which we would like you to consider is that we frequently set up user accounts on networks and install data intercept devices to perform a "test tap" under our own consent. This is generally done as a means of verifying that the location on the network and the filter set would be appropriate for an anticipated or existing intercept Order. In the event that we are doing a "test tap" under consent, looking for our own mail, etc, and inadvertently capture something outside our consent, such as another persons mail, what are our options? Is it a violation of TIII if the interception is not intentional and we do not disclose or endeavor to disclose the information to anyone? May we destroy the information and simply not disclose it to anyone?

Issue IV

Random Access Memory RAM

In relation to the "testing" of network placement and filters, it is generally a technical requirement to install the device with appropriate filters set and initiate the capture process. It may be hours or days before a determination can be made as to the functional operation of the collection. During these first few hours or days, the technical representatives of the FBI, Electrical Engineers, Electronics Engineers, Technically Trained Special Agents and others may frequently examine collected data to determine the efficacy of the installation. In relation to the time period from installation to the verification of proper function, the following question is posed for your consideration. Is there a significant legal difference between Random Access Memory (RAM), that which is not retained when power is removed, and of a hard-drive or floppy disk which retains the data. The thought process here in the DITU being that: during the period of time from the installation to the verification of proper function, the data could be directed to remain in RAM and not be forwarded to a permanent media. Technical representatives could then examine the collected data for proper filtering and

assure that the collection is operating within the scope of the Order.

If the collection appears technically correct, it could then be re-directed from RAM to permanent media and the intercept initiated. If not, the data could be examined in RAM by Computer Programmers/Engineers to determine a filtering change or software patch necessary to effect the Court Ordered intercept. The data in RAM would not be retained by the computer on power-off.

By directing collected data to remain only in RAM, we may gain both the ability to troubleshoot installations and to assure that the data is not written to "storage media" nor recoverable from any media.

64-1
67E-1

From: [redacted]
To: [redacted] THOMAS, MARCUS C
Date: Wed, Apr 12, 2000 5:53 PM
Subject: ISP INTERCEPTS E-MAIL

See the attached. After you all get a chance to review my initial thoughts regarding your questions/issues, let's then plan to sit down and talk.

TX

[redacted]

Doc. #7

4/12/2000

TO: Marcus Thomas
[redacted]

FROM: [redacted]

RE: Internet/E-Mail Intercepts

b6-1
b7C-1

This is in response to [redacted] E-mail of 4/11 regarding the captioned matter.

The following are some preliminary reactions and thoughts. They are not necessarily final legal answers or guidance. They are offered to stimulate further consideration on all of our parts. As was suggested in the E-mail, we all need to sit down in the very near future and take a little time to talk about our intercept approaches, as well as what we must do when they unintentionally go astray.

Background:

We need to start with a few high-level and familiar thoughts, because they form a background and context for the subsequent discussion. As we are all aware and appreciate, electronic surveillance is a very sensitive investigative (and intelligence/counterintelligence) technique.[1] As such, for over 30 years, it has been carefully regulated by and through statutory regimes at both the Federal and State levels -- which regimes, in many instances, contain provisions that are very specific, and which contain dictates that are quite detailed in their procedural/administrative aspects. On its face, the language of these regimes, as written by the Congress, is essentially black and white, and generally is unforgiving: one complies with the statutes or, alternatively, violates them. In enacting these regimes, Congress sought to balance and advance privacy and effective law enforcement. Moreover, given the sensitivity of this technique, electronic surveillance has been the subject of on-going scrutiny by Congressional oversight committees, the press, privacy groups, and the public. In short, there are few, if any, investigative techniques that are (and have been) subjected to such heightened scrutiny. And there are few, if any, investigative techniques that garner (and have garnered in the past) such vehement criticism when errant surveillances or missteps (be they intentional or unintentional) occur.

While, as noted above, the electronic surveillance laws are often specific and detailed in their provisions, generally they do not address the precise aspects of how, technical speaking, the "intercept" is to occur. Congress eschewed doing so because it would be a bad idea to try to delineate all the various potential interception methodologies/approaches. To do so would infringe upon Executive Branch prerogatives in "executing" the laws. And, it would get into sensitive intercept sources and methods, etc. Nevertheless, both the Congress and the courts have

[1] While we in our particular area of law enforcement are so close to this matter that we literally live and breathe electronic surveillance, to others (especially those outside of law enforcement), *any electronic surveillance is a big thing!*

an extremely keen interest in making sure that several things are being attended to by the Executive Branch in conducting electronic surveillance searches and seizures: (1) that illegal, unconstitutional searches are not occurring (i.e., that no searches of persons' communications are occurring without probable cause/warrant/emergency); and (2) that the spirit/intent/letter of the electronic surveillance laws (as implementers of constitutional law -- at least to a degree) are being carried out carefully and judiciously. One aspect of this involves the requirement that such surveillances only be approved with high-level departmental approval and with on-going Departmental legal/administrative oversight.

Interceptions of the "Older" Communications Technology

It is probably fair to say that, historically, Congress has been of the opinion (and correctly so) that, for law enforcement, effecting a lawful interception was not a particularly problematic endeavor. Typical wire line service lent itself to reasonably easy segregation of a target's communications to the target line,[2] and thus to concomitantly effecting lawful (and effective technically-targeted) interceptions. With other identifiers (ESNs, MINs, Cap Codes, etc.) being available, accurately targeted interceptions of cellular phones and pagers could likewise be effected by law enforcement. Importantly, Congress understood that, in order to effect accurate interceptions, law enforcement would seek and obtain assistance from electronic communication service providers (ECSPs) and/or others to properly conduct the intercept ("...upon request [of an ECSP, it shall] furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception ... with a minimum of interference with the services [the ECSP is according to] the person whose communications are to be intercepted"). 2518 U.S.C. 2518(4). Until 1994 (*see* below), there is no clear indication, in the statutes or otherwise, that Congress ever understood *interception accuracy* to be an issue for law enforcement.

Where potential "over-acquisitions" could arise, Congress, privacy groups, and others have homed in and taken an interest. For example, with regard to pen register/DNRs, Congress and others have been concerned about certain (but not all) post cut-through dialing -- i.e., certain dialing that arguably constitutes a substantive communication -- even though related to the target individual (as opposed to communications of others). In this regard, Congress, as part of the CALEA legislation, specified in 18 U.S.C. 3121(c) that law enforcement "shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing or signaling information utilized in call processing." Similarly, under CALEA's assistance capability requirements, Congress specified, as a statutory requirement as part of the interception capability, that telecommunications carriers meet their obligation "in a manner that

---

[2] One possible exception being "party-line" service, which by now is pretty rare. Its unclear exactly what Congress would think about such party-line-related intercepts. Presumably, minimization could be employed to parse the target subscriber's calls. But, at the end of day, under the statutory regime/language, the telephonic communications being targeted for interception would, in fact, be occurring over the properly-targeted telephone line/facility. Here, law enforcement would, at least, be on the correct line/facility that had been authorized for interception by the court.

protects ... the privacy and security of communications and call-identifying information not authorized to be intercepted...." 47 U.S.C. 1002(a)(4)(A).

Internet and E-mail Service Providers

Both Internet Service Providers (ISPs) and E-mail service providers are comprehended within the term "providers of 'electronic communication service'" under the ECPA and Title III/FISA. *See, e.g.*, 18 U.S.C. 2510(15). Moreover, certain facets of E-mail/ISP service, at least with regard to the acts of transmitting and routing wire/electronic communications, can also constitute activity of a "telecommunications carrier," thereby subjecting the communications/carrier to the provisions of CALEA. *See* 47 U.S.C. 1001(8). Accordingly, certainly under the ECPA/Title III/FISA (and perhaps under CALEA), such electronic communication service providers are mandated to afford all the necessary assistance to properly effectuate an interception of electronic communications. Consequently, whenever there is an electronic surveillance order, and whenever there are any questions about "standard/non-standard transmission control(s)," "protocols," or any other technical information matter of consequence in properly and accurately effecting electronic surveillance, these service providers are duty-bound to work with us in properly and lawfully effecting the surveillance order.

Internet/E-mail Interceptions

In the referenced DITU E-mail, it is explained that certain Etherpeek and Carnivore "filters" are utilized to (hopefully) capture data (and only that data) authorized for interception in an electronic surveillance order or pursuant to consent. The E-mail mentions that, on occasion, when non-standard implementations have been encountered, data outside the court order or consent have been captured and processed inadvertently. DITU then presents several issues for examination. In the first two, DITU (1) seeks guidance as to formulating guidelines for reacting to such inadvertent interceptions and (2) whether additional examination of such non-authorized data is permitted to remedy the errant collection/filtering efforts.

As noted in the background comments, the electronic surveillance statutes speak at a rather high level, and are essentially black and white in nature -- with one either complying with the law or facially violating it. The Title III statutes, generally speaking, are not "specific intent" statutes. That is, one does not need to have *special* or *particular bad intention* or *motive* to facially violate the law. Further, since the protection of personal communications privacy is a key facet of the statutory purpose and regime, any unauthorized interception of another's communications is a matter of concern (at a minimum). Indeed, some might argue that the government's unauthorized interception of such communications is even more problematic.

Historically, as a matter of Departmental practice/policy, unauthorized interceptions (be they of the subject of the interception or others) have been taken seriously by DOJ (and by the FBI for that matter). When detected, DOJ has advised AUSAs to (1) file a pleading with the court explaining the unintentional/intentional act and to (2) seal the unauthorized intercepted communications with the court, in order to prevent further harm such as subsequent use or disclosure (*see* 18 U.S.C. 2511(1)(c)(d), 2515). Such unauthorized interceptions not only can

violate a citizen's privacy but also can seriously "contaminate" ongoing investigations. In addition, DOJ could also counsel the AUSA to recommend/not recommend to the court whether or not the person(s) who communications were improperly intercepted should be notified.

Interestingly, under Section 2511(2)(a)(ii), while Title III specifies that "no [criminal] cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification [under Title III]," there is no similar explicit protection for law enforcement personnel under this provision. Now, practically speaking, there is virtually no chance that law enforcement officers acting in good faith, pursuant to a court order, are going to be criminally prosecuted (or even investigated)! As to civil liability, under 18 U.S.C. 2520(d), Title III states that "a good faith reliance on ... a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization... is a complete defense against any civil or criminal action brought under [Title III] or any other law." So, here too, law enforcement personnel should be immune, practically speaking, from any liability. (Further, even if (in a semi-egregious case) liability were to be found, it would almost certainly fall to the agency -- not the agent/support personnel.) However, the FBI itself routinely does conduct OPR-type inquiries, from an administrative perspective, in order to determine the nature/cause, etc. of any investigative missteps or errors which facially violate a law, with an eye toward preventing future reoccurrences, etc.

In a similar fashion, missteps under FISA lead to mandatory reporting to the President's Foreign Intelligence Advisory Board (PFIAB), and such errancies must be reported/explained/justified to Congress.

Issue #1:

In short, then, as to the first issue, upon detecting an inadvertent, unauthorized (unlawful) interception:

A) the technical effort that is causing the mistake should be stopped immediately (and not re-instituted until advised to do so by the supervising attorneys);
B) the error should be reported immediately to the FBI substantive case personnel in the field/headquarters (as appropriate), to the field office TA and CDC, and to the respective AUSA/OIPR supervisory attorney (who, in turn, will presumably advise the court);
C) the reporting as to the errant interception should be careful and clear so that those to whom it is reported will fully understand what happened; the reporting should not include any substantive aspect of the *content* of the communication that may have been gleaned; and
D) the unauthorized intercepted material should be segregated immediately as a prelude to formal sealing with the court.

Issue #2:

As to "examining" the unauthorized intercepted data (albeit for the sole purpose of determining why the filters failed and what changes need to be made), this is a very delicate and potentially

problematic area. It would appear that continuing to look at (examine and "use") the substantive content/plain text of the material that was not authorized for interception would most aggravate Title III's concerns/dictates (*see* Sections 2511 and 2515), and most likely would *heighten* the legal problem in the minds of the Department, FBI-OPR, the court, Congress, privacy groups, the public, etc. If, on the other hand, there is some way of looking at the signaling, programing, protocols, etc. *in a raw/unintelligible state (I can amplify later)*, this might be okay if (1) it is for the sole purpose of determining why the filters failed and what changes need to be made, and if (2) it is approved by the AUSA/OIPR (and/or the court if the AUSA/OIPR believe warranted -- such court permission in this area would presumably be preferable from the perspective of legal protection for our technical people). Another thought I would strongly encourage is to engage the ISP. That is, if there is a technical (filter) failure problem regarding the interception, it would appear to be much much more preferable for the ISP to try to fix it (even with us coaching and/ or guiding technically from afar). The reason for fully utilizing the ISP is the existing mandate for their assistance, etc. under the law, and because of the "cover" it affords us legally, politically, and perceptionally.

Issue #3:

DITU poses a similar issue as to one its own "test" accounts where an inadvertent, unauthorized interception occurs. Again, we have to be very careful here, even where "testing" is our activity, because the potential harm/violation of privacy is arguably the same. Somehow, when we test, we have to go out of our way to avoid tripping over innocent third party communications. I am not sure how we can proceed to test without inadvertently intercepting the communications of others, but we really need to try. Perhaps, we can explain our testing requirement to the ISP and get them to test our filters, etc. for us, since it is *their* network, and since *they* administrate it, etc. anyway. I would really encourage using the ISPs for many reasons, not the least of which is to make them aware of us popping around in their network to conduct testing, etc.

Issue #4:

DITU asks whether interception collections effected in Random Access Memory (RAM) (rather than permanent media) make any significant legal difference. In short, I would say probably not as a purely legal matter, inasmuch as an unauthorized interception is, after all, an unauthorized interception. Now, having said that, it may make some feel better that the potential for ongoing "use" and "disclosure"(through some permanent storage media) may be somewhat reduced -- but I don't think this is the path to take. As alluded to above, I would opt for more controlled testing and utilizing service providers as much as possible to create some insulation between us and the subscriber public where inadvertent interceptions might arise in the course of our trying out our filters, etc.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

3 Pages were not considered for release as they are duplicative of DOC #1, OGC/TECHNOLOGY LAW UNIT FILE

_____ Page(s) withheld for the following reason(s): (PAGES 155-157)

_____

_____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #8 (Pages 614-616)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

66-1
67C-1

FBI Using Internet Wiretap System (washingtonpost.com)

By John Schwartz
Washington Post Staff Writer
Tuesday, July 11, 2000; Page A1

The FBI has deployed an automated system to wiretap the Internet, giving authorities a new tool to police cyberspace but drawing concerns among civil libertarians and privacy advocates about how it might be used.

The new computer system, dubbed "Carnivore" inside the FBI because it rapidly finds the "meat" in vast amounts of data, was developed at FBI computer labs in Quantico, Va., and has been used in fewer than 50 cases so far.

But that number is sure to rise, said Marcus Thomas, chief of the FBI's cyber-technology section at Quantico. "In criminal situations there's not yet been a large call for it," he said, but the bureau already has seen "growth in the rate of requests."

Civil liberties groups said the new system raises troubling issues about what constitutes a reasonable search and seizure of electronic data. In sniffing out potential criminal conduct, the new technology also could scan private information about legal activities.

"It goes to the heart of how the Fourth Amendment and the federal wiretap statute are going to be applied in the Internet age," said Marc Rotenberg, head of the Washington-based Electronic Privacy Information Center.

The new system, which operates on off-the-shelf personal computers, takes advantage of one of the fundamental principles of the Internet: that virtually all such communications are broken up into "packets," or uniform chunks of data. Computers on the Internet break up e-mail messages, World Wide Web site traffic and other information into pieces and route the packets across the global network, where they are reassembled on the other end.

FBI programmers devised a "packet sniffer" system that can analyze data flowing through computer networks to determine whether it is part of an e-mail message or some other piece of Web traffic.

The ability to distinguish between packets allows law enforcement officials to tailor their searches so that, for example, they can examine e-mail but leave alone a suspect's online shopping activities. The system could be tuned to do as little as monitoring how many e-mail messages the suspect sends and to whom they are addressed ù the equivalent of a telephone "pen register," which takes down telephone numbers being called without grabbing the content of those calls.

"That's the good news," said James Dempsey, an analyst with the Center for Democracy and Technology, a Washington high-tech policy group. "It is a more discriminating device" than a full wiretap, he said.

But Dempsey expressed worries about the new system, which would be

Doc #9

b6-1
b7C-1

from pen-register data to full wiretaps with court authorization. "It's not an increase in our authority; it doesn't present a change of volume in what we do," he said.

66-1
67c-1

FBI e-mail Snooping Device Attacked

July 11, 2000

Filed at 7:26 p.m. EDT
By The Associated Press
WASHINGTON (AP) -- Civil liberties and privacy groups railed Tuesday against a new system designed to allow law enforcement agents to intercept and analyze huge amounts of e-mail in connection with an investigation.
The system, called ``Carnivore,'' was first hinted at on April 6 in testimony to a House subcommittee. Now the FBI has it in use.
When Carnivore is placed at an Internet Service Provider, it scans all incoming and outgoing e-mails for messages associated with the target of a criminal probe.
In a letter addressed to two members of the House subcommittee that deals with Fourth Amendment search-and-seizure issues, the American Civil Liberties Union argued that the system breaches the Internet provider's rights and the rights of all its customers by reading both sender and recipient addresses, as well as subject lines of e-mails, to decide whether to make a copy of the entire message.
Further, while the system is plugged into the Internet provider's systems, it is controlled solely by the law enforcement agency. In a traditional wiretap, the tap is physically placed and maintained by the telephone company.
``Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers, with the 'assurance' that the FBI will record only conversations of the specified target,'' read the letter. ``This 'trust us, we are the government' approach is the antithesis of the procedures required under our wiretapping laws.''
Barry Steinhardt, associate director of the ACLU, said citizens shouldn't trust that such a sweeping data-tap will only be used against criminal suspects. And even then, he said, the data mined by Carnivore, particularly subject lines, is already intrusive.
``Law enforcement should be prohibited from installing any device that allows them to intercept communications from persons other than the target,'' Steinhardt said in an interview. ``When conducting these kinds of investigations, the information should be restricted to only addressing information.''
A spokeswoman for Rep. Charles T. Canady, R-Fla., who heads the Constitution subcommittee, said that the congressman had no immediate comment on the letter.
In testimony to Canady's subcommittee, Robert Corn-Revere, a lawyer at the Hogan & Hartson law firm in Washington, said that he represented

Doc #10

b6-1
b7C-1

an Internet provider that refused to install the Carnivore system. The provider was placed in an ``awkward position,'' Corn-Revere said, because the company feared suits from customers unhappy with the government looking in to all the e-mail.

``It was acknowledged (by the government) that Carnivore would enable remote access to the ISP's network and would be under the exclusive control of government agents,'' Corn-Revere said.

Corn-Revere told the committee that current law is insufficient to deal with Carnivore's potential and that the Internet provider lost their court battle in part because of the Internet's connection to telephone lines, and that the law was stretched to cover the Internet as well.

Corn-Revere would not reveal the name of his client, and the client lost the case. He said that the FBI has been using Carnivore since early this year.

James X. Dempsey, senior staff counsel at the Center for Democracy and Technology, said that the main problem with Carnivore is it's mystery.

``The FBI is placing a black box inside the computer network of an ISP,'' Dempsey said. ``Not even the ISP knows exactly what that gizmo is doing.''

But Dempsey said that Internet providers contributed to the problem, by saying that current technology does not allow the Internet provider to sort out exactly what the government is entitled to get under a search warrant. The carriers complained that they had to give everything to the FBI.

``The service providers said they didn't know how to comply with court orders,'' Dempsey said. ``By taking that position, they have hurt themselves, putting themselves into a box.''

Marcus Thomas, who heads the FBI's Cyber Technology Section, told the Wall Street Journal that the bureau has about 20 Carnivore systems, which are PCs with proprietary software. He said Carnivore meets current wiretapping laws, but is designed to keep up with the Internet.

``This is just a specialized sniffer,'' Thomas told the Journal, which first reported details about Carnivore.

Encrypted e-mail, done with an e-mail encoding program like PGP, still stays in code on Carnivore, and it's up to agents to decode it.

Dempsey has a possible solution to the problem, though one that's probably unlikely -- show everyone what it does and how it does it, allowing Internet providers to install the software themselves.

``The FBI should make this gizmo an open-source product,'' he said. ``Then the secret is gone.''

On the Net: Federal Bureau of Investigation: http://www.fbi.gov

66-1
67c-1

American Civil Liberties Union: http://www.aclu.org
Center for Democracy and Technology: http://www.cdt.org
Pretty Good Privacy (PGP): www.pgp.com

Jul 11 2000 11:55 P.01

WALL STREET ARTICLE

[redacted] b4-1

FACSIMILE COVER SHEET
FAX NUMBER [redacted]

Number of Pages 6 *(Including Cover)*

Date: 7/11/00

To: Marcus Thomas

Phone:

FAX: 703-632-6091

From: [redacted] b6-2

Phone: 703-[redacted] b7C-2

Comments:

DOC #11

FBI's system to covertly search e-mail raises privacy, legal issues

By Neil King Jr. and Ted Bridis
THE WALL STREET JOURNAL

WASHINGTON, July 11 — The U.S. Federal Bureau of Investigation is using a superfast system called Carnivore to covertly search e-mails for messages from criminal suspects.

© COMPLETE STORY

ESSENTIALLY A PERSONAL COMPUTER stuffed with specialized software, Carnivore represents a new twist in the federal government's fight to sustain its snooping powers in the Internet age. But in employing the system, which can scan millions of e-mails a second, the FBI has upset privacy advocates and some in the computer industry. Experts say the system opens a thicket of unresolved legal issues and privacy concerns.

The FBI developed the Internet wiretapping system at a special agency lab at Quantico, Va., and dubbed it Carnivore for its ability to get to "the meat" of what would otherwise be an enormous quantity of data. FBI

technicians unveiled the system to a roomful of astonished industry specialists here two weeks ago in order to steer efforts to develop standardized ways of complying with federal wiretaps. Federal investigators say they have used Carnivore in fewer than 100 criminal cases since its launch early last year.

Word of the Carnivore system has disturbed many in the Internet industry because, when deployed, it must be hooked directly into Internet service providers' computer networks.

Word of the Carnivore system has disturbed many in the Internet industry because, when deployed, it must be hooked directly into Internet service providers' computer networks.

Word of the Carnivore system has disturbed many in the Internet industry because, when deployed, it must be hooked directly into Internet service providers' computer networks. That would give the government, at least theoretically, the ability to eavesdrop on all customers' digital communications, from e-mail to online banking and Web surfing.

The system also troubles some Internet service providers, who are loath to see outside software plugged into their systems. In many cases, the FBI keeps the secret Carnivore computer system in a locked cage on the provider's premises, with agents making daily visits to retrieve the data captured from the provider's network. But legal challenges to the use of Carnivore are few, and judges' rulings remain sealed because of the secretive nature of the investigations.

Internet wiretaps are conducted only under state or federal judicial order, and occur relatively infrequently. The huge majority of wiretaps continue to be the traditional telephone variety, though U.S. officials say the use of Internet eavesdropping is growing as everyone from drug dealers to potential terrorists begins to conduct business over the Web.

The FBI defends Carnivore as more precise than Internet wiretap methods used in the past. The bureau says the system allows investigators to tailor an intercept operation so they can pluck only the digital traffic of one person from among the stream of millions of other messages. An earlier version, aptly code-named Omnivore, could suck in as much as to six gigabytes of data every hour, but in a less discriminating fashion.

Still, critics contend that Carnivore is open to abuse.

Mark Rasch, a former federal computer-crimes prosecutor, said the nature of the surveillance by Carnivore raises important privacy questions, since it analyzes part of every snippet of data traffic that flows past, if only to determine whether to record it for police.

"It's the electronic equivalent of listening to everybody's phone calls to see if it's the phone call you should be monitoring," Mr. Rasch said. "You develop a tremendous amount of information."

"It's the electronic equivalent of listening to everybody's phone calls to see if it's the phone call you should be monitoring," Mr. Rasch said. "You develop a tremendous amount of information."

Others say the technology dramatizes how far the nation's laws are lagging behind the technological revolution. "This is a clever way to use old telephone-era statutes to meet new challenges, but clearly there is too much latitude in the current law," said Stewart Baker, a lawyer specializing in telecommunications and Internet regulatory matters.

Robert Corn-Revere, of the Hogan & Hartson law firm here, represented an unidentified Internet service provider in one of the few legal fights against Carnivore. He said his client worried that the FBI would have access to all the e-mail traffic on its system, raising dire privacy and security concerns. A federal magistrate ruled against the company early this year, leaving it no option but to allow the FBI access to its system.

"This is an area in desperate need of clarification from Congress," said Mr. Corn-Revere.

"Once the software is applied to the ISP, there's no check on the system," said Rep. Bob Barr (R., Ga.), who sits on a House judiciary subcommittee for constitutional affairs. "If there's one word I would use to describe this, it would be 'frightening.'"

Marcus Thomas, chief of the FBI's Cyber Technology Section at Quantico, said Carnivore represents the bureau's effort to keep abreast of rapid changes in Internet communications while still meeting the rigid demands of federal wiretapping statutes. "This is just a very specialized sniffer," he said.

He also noted that criminal and civil penalties prohibit the bureau from placing unauthorized wiretaps, and any information gleaned in those types of criminal cases would be thrown out of court. Typical Internet wiretaps last around 45 days, after which the FBI removes the equipment. Mr. Thomas said the bureau usually has as many as 20 Carnivore systems on hand, "just in case."

FBI experts acknowledge that Carnivore's monitoring can be stymied with computer data such as e-mail that is scrambled using powerful encryption technology. Those messages still can be captured, but law officers trying to read the contents are "at the mercy of how well it was encrypted," Mr. Thomas said.

Most of the criminal cases where the FBI used Carnivore in the past 18 months focused on what the bureau calls "infrastructure protection," or the hunt for hackers, though it also was used in counterterrorism and some drug-trafficking cases.

TOP WSJ STORIES ON MSNBC

STORY AOL's assault on Latin America hits a snag with local providers
STORY Deutsche Telekom makes overtures to acquire VoiceStream Wireless
STORY Dell halts the sale of WebPC line
STORY Microsoft aims to sell developers on its new computing platform
STORY Fast-food franchise bank loans fall out of favor with lenders
STORY Ready to list? Selecting where has become tricky in Europe

TOP BUSINESS NEWS

STORY Deutsche Telekom makes overtures to acquire VoiceStream Wireless
STORY Tipping the scales both ways in Microsoft case
STORY Yahoo, with new 'vision,' set to report earnings
STORY Lobbyists go to battle over spectrum
STORY Dell halts the sale of WebPC line

Marcus C. Thomas

From: [redacted]
To: [redacted] Ed Allen <eallen@fbi.gov>; Marcus [redacted] <mthomas@ibiacademy.edu> [redacted]
Sent: Tuesday, July 11, 2000 10:05 AM
Subject: Carnivore article .... !!

All FYI ... if you are not already aware !!! Source is UK ZDnet page !!

[redacted]

News Burst: FBI uses covert email surveillance system

Tue, 11 Jul 2000 16:21:36 GMT

Will Knight

A super-fast scanning system nicknamed 'Carnivore' is being used by the FBI to covertly search through email messages, says the Wall Street Journal

America's Federal Bureau of Investigation (FBI) is using a super-fast email scanning system dubbed "Carnivore" to covertly trawl through email messages in order to capture suspected criminals, reports the Wall Street Journal Tuesday.

The revelations have caused a furore among privacy and security advocates, because it requires a direct connection to a commercial ISP's network, giving the authorities, in theory, access to all Internet communications.

Carnivore is reportedly nothing more than a personal computer fitted with special software capable of scanning millions of emails in a second.

According to the WSJ's report Carnivore, which was launched last year, has been used to gather evidence in fewer than 100 criminal cases.

Doc #12

07/11/2000

FBI e-mail Snooping Device Attacked

By D. IAN HOPPER
.c The Associated Press

WASHINGTON (AP) - Civil liberties and privacy groups are railing against a new system designed to allow law enforcement agents to intercept and analyze huge amounts of e-mail in connection with an investigation.

The system, called ``Carnivore,'' was first hinted at on April 6 in testimony to a House subcommittee. Now the FBI has it in use.

When Carnivore is placed at an Internet service provider, it scans all incoming and outgoing e-mails for messages associated with the target of a criminal probe.

In a letter addressed to two members of the House subcommittee that deals with Fourth Amendment search-and-seizure issues, the American Civil Liberties Union argued that the system breaches the Internet provider's rights and the rights of all its customers by reading both sender and recipient addresses, as well as subject lines of e-mails, to decide whether to make a copy of the entire message.

Further, while the system is plugged into the Internet provider's systems, it is controlled solely by the law enforcement agency. In a traditional wiretap, the tap is physically placed and maintained by the telephone company.

``Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers, with the 'assurance' that the FBI will record only conversations of the specified target,'' read the letter. ``This 'trust us, we are the government' approach is the antithesis of the procedures required under our wiretapping laws.''

Barry Steinhardt, associate director of the ACLU, said citizens shouldn't trust that such a sweeping data-tap will only be used against criminal suspects. And even then, he said, the data mined by Carnivore, particularly subject lines, are already intrusive.

``Law enforcement should be prohibited from installing any device that allows them to intercept communications from persons other than the target,'' Steinhardt said in an interview. ``When conducting these kinds of investigations, the information should be restricted to only addressing information.''

A spokeswoman for Rep. Charles T. Canady, R-Fla., who heads the House Judiciary subcommittee on the Constitution, said the congressman had no comment on the letter.

In testimony to Canady's subcommittee, Robert Corn-Revere, a lawyer at the Hogan & Hartson law firm in Washington, said he represented an Internet provider that refused to install the Carnivore system. The provider was placed in an ``awkward position,'' Corn-Revere said, because the company feared suits from customers unhappy with the government looking into all

DOC #13

the e-mail.

``It was acknowledged (by the government) that Carnivore would enable remote access to the ISP's network and would be under the exclusive control of government agents," Corn-Revere said.

Corn-Revere told the committee that current law is insufficient to deal with Carnivore's potential and that the Internet provider lost its court battle in part because of the Internet's connection to telephone lines, and that the law was stretched to cover the Internet as well.

Corn-Revere would not reveal the name of his client, and the client lost the case. He said the FBI has been using Carnivore since early this year.

James X. Dempsey, senior staff counsel at the Center for Democracy and Technology, said the main problem with Carnivore is its mystery.

``The FBI is placing a black box inside the computer network of an ISP," Dempsey said. ``Not even the ISP knows exactly what that gizmo is doing."

But Dempsey said Internet providers contributed to the problem, by saying that current technology does not allow the Internet provider to sort out exactly what the government is entitled to get under a search warrant. The carriers complained that they had to give everything to the FBI.

``The service providers said they didn't know how to comply with court orders," Dempsey said. ``By taking that position, they have hurt themselves, putting themselves into a box."

Marcus Thomas, who heads the FBI's cybertechnology section, told the Wall Street Journal that the bureau has about 20 Carnivore systems, which are PCs with proprietary software. He said Carnivore meets current wiretapping laws, but is designed to keep up with the Internet.

``This is just a specialized sniffer," Thomas told the Journal, which first reported details about Carnivore.

Encrypted e-mail, done with an e-mail encoding program like PGP, still stays in code on Carnivore, and it's up to agents to decode it.

Dempsey has a possible solution to the problem, though one that's probably unlikely - show everyone what it does and how it does it, allowing Internet providers to install the software themselves.

``The FBI should make this gizmo an open-source product," he said. ``Then the secret is gone."

On the Net: Federal Bureau of Investigation: http://www.fbi.gov

American Civil Liberties Union: http://www.aclu.org

Center for Democracy and Technology: http://www.cdt.org

Pretty Good Privacy (PGP): www.pgp.com

AP-NY-07-12-00 0812EDT

FBI's Internet Wiretaps Raise Privacy Concerns

By John Schwartz
Washington Post Staff Writer
Tuesday, July 11, 2000; Page A01

• Privacy Special Report
• What's Your Opinion?
E-Mail This Article
Printer-Friendly Version

The FBI has deployed an automated system to wiretap the Internet, giving authorities a new tool to police cyberspace but drawing concerns among civil libertarians and privacy advocates about how it might be used.

The new computer system, dubbed "Carnivore" inside the FBI because it rapidly finds the "meat" in vast amounts of data, was developed at FBI computer labs in Quantico, Va., and has been used in fewer than 50 cases so far.

But that number is sure to rise, said Marcus Thomas, chief of the FBI's cyber-technology section at Quantico. "In criminal situations there's not yet been a large call for it," he said, but the bureau already has seen "growth in the rate of requests."

Civil liberties groups said the new system raises troubling issues about what constitutes a reasonable search and seizure of electronic data. In sniffing out potential criminal conduct, the new technology also could scan private information about legal activities.

"It goes to the heart of how the Fourth Amendment and the federal wiretap statute are going to be applied in the Internet age," said Marc Rotenberg, head of the Washington-based Electronic Privacy Information Center.

The new system, which operates on off-the-shelf personal computers, takes advantage of one of the fundamental principles of the Internet: that virtually all such communications are broken up into "packets," or uniform chunks of data. Computers on the Internet break up e-mail messages, World Wide Web site traffic and other information into pieces and route the packets across the global network, where they are reassembled on the other end.

FBI programmers devised a "packet sniffer" system that can analyze data flowing through computer networks to determine whether it is part of an e-mail message or some other piece of Web traffic.

The ability to distinguish between packets allows law enforcement officials to tailor their searches so that, for example, they can examine e-mail but leave alone a suspect's online shopping activities. The system could be tuned to do as little as monitoring how many e-mail messages the suspect sends and to whom they are addressed--the equivalent of a telephone "pen register," which takes down telephone numbers being called without grabbing the content of those calls.

"That's the good news," said James Dempsey, an analyst with the Center for Democracy and Technology, a Washington high-tech policy group. "It is a more discriminating device" than a full wiretap, he said.

But Dempsey expressed worries about the new system, which would be installed at the offices of a suspect's Internet service provider. Just as the device could be used to fine-tune a search, it also could used for broad sweeps of data. "The bad news is that it's a black box the government wants to insert into the premises of a service provider. Nobody knows that it does what the government claims it would do," Dempsey said.

Existence of the Carnivore system was discussed in a Wall Street Journal article yesterday, which reported that the FBI showed the system to telecommunications industry experts two weeks ago.

Albert Gidari, a lawyer who works for the wireless industry, was present at the FBI demonstration. He said the FBI's announcement was intended to counter industry assertions that it would be very difficult to provide the kind of pen-register wiretap capability that the agency wants.

Since the demonstration, Gidari said, one faction within telecommunications industry was pleased with the FBI's efforts. But Gidari said the other faction was saying: "Wait a minute--what are the liability issues? What are the privacy issues? We don't want third-party software on our system."

Although Congress has passed legislation requiring telephone companies to make their developing high-tech networks easy to wiretap, Gidari is one of a large number of industry experts who believe the law does not apply to wiretapping the Internet. "The FBI overreaches in everything they do," said Gidari, who is president of G-Savvy, an Internet consulting company.

A former federal prosecutor sounded a more supportive tone. "If what it does is it helps comply with wiretaps, and it helps minimize what you're getting--to help get what the court authorizes you to get--there's nothing wrong with it," said Mark Rasch, now a security consultant with Reston-based Global Integrity.

Still, Rasch said the technology raised questions that have yet to be fully explored by law enforcement. The PC robocop examines all packets coming through a computer network but gives live law enforcement officers only those packets related to the subject of the investigation.

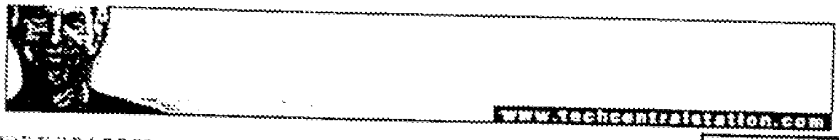
"The stuff that is examined only by a computer and not by a human being--was that information searched?" Rasch asked. He then suggested

an answer: "It is a search, but it is to an extent less invasive than it would be if you did not use this technology."

The first news of Carnivore actually came in April during congressional testimony by Washington lawyer Robert Corn-Revere, who represented an Internet service provider that tried to resist attaching the system to its network. Corn-Revere suggested that such a system could be used to track dissidents and journalists online. "There are some human rights issues here," he said.

But Thomas of the FBI said there is nothing mysterious about the new device. "This is an effort on the FBI's part to keep pace with changes in technology--to maintain our ability" to lawfully intercept everything from pen-register data to full wiretaps with court authorization. "It's not an increase in our authority; it doesn't present a change of volume in what we do," he said.

◀ Previous Article Back to the top Next Article ▶



OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of Doc. #4, OGC/TECHNOLOGY LAW UNIT FILE (PGS. 162 + 163)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages: DOCUMENT #15, PGS. 1+2 (Pages 636-637)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Get credit for that old IBM PC, laptop

BY PAULA SHAKI TRIMBLE

Federal agencies will be able to obtain credit toward the purchase of new IBM Corp. PCs and laptops by donating their old computers to charity via a unique governmentwide contract.

The Department of Veterans Affairs Special Services office and the Air Force Medical Logistics Office awarded a decentralized blanket purchase agreement last week to iGov.com, an online computer equipment reseller, that would allow government customers to receive a trade-in allowance for their older IBM equipment at the time of purchase.

Agencies could receive a $300 credit for IBM PCs that have 486 or faster processors and are Year 2000-compliant, said Corinne Lingebach, iGov.com's program manager for the Technical Refresh and Trade-In program, which is open to all government agencies and runs through Oct. 8, 2002. The credit can be applied to the purchase of a new computer. Agencies could receive a $500 credit for each laptop turned in.

The BPA, based on iGov.com's General Services Administration schedule contract, "is a better value, and it enhances programs we already have," said government contracting officer Mary Rust. "Only iGov offers the trade-in, so it's unique."

The contract guarantees iGov.com at least $500,000 in sales, but the company anticipates more than $25 million in sales over the life of the contract, said Brad Mack, iGov.com's vice president of sales.

In the future, Rust hopes to add other types of computer equipment to the program. Although there are no other contracts that offer trade-in credits, Rust's office does offer other unique programs that benefit schools and other charities.

iGov.com partnered with Gifts In Kind International, an Alexandria, Va.-based charity organization, to refurbish federal agencies' obsolete systems and deliver them to charitable organizations.

Agencies can specify a charity or allow Gifts In Kind to choose the charity that will receive the computer. Gifts In Kind's Recycle Technology program, which supplies refurbished computers to needy organizations, has donated about 20,000 computers a year to nonprofit organizations since it started in 1994, said Doug McAllister, Gifts In Kind's director of marketing and communications. "Computers and technology are high on the needs list for charity," McAllister said.

Responsibility for deleting classified information from computer hard drives or removing the hard drives themselves rests with the agency trading in the equipment, Mack said. ■

ACLU: Block FBI e-snoops

BY DAN VERTON

The American Civil Liberties Union appealed to Congress last week to protect Americans from unreasonable searches and seizures on the Internet in light of recent revelations that a new monitoring tool could enable the FBI to intercept the e-mail of law-abiding citizens.

In a letter to the House Judiciary Committee's Constitution Subcommittee, ACLU director Laura Murphy argued that the FBI's new Carnivore e-mail surveillance system gives federal law enforcement officers access to the e-mail of every customer of an Internet service provider and the e-mail of every person who communicates with them.

"The Carnivore system gives law enforcement e-mail interception capabilities that were never contemplated when Congress passed the Electronic Communications Privacy Act" in 1986, Murphy stated in the letter. "The ACLU urges the subcommittee to accelerate its consideration of the application of the Fourth Amendment in the Digital Age."

The Fourth Amendment to the Constitution protects the public from unreasonable searches and seizures.

Attorney General Janet Reno said July 13 that she is now looking into the allegations. "When we develop new technology, when we apply the Constitution, I want to make sure that we apply it in a consistent and balanced way," Reno said.

Robert Corn-Revere, an Internet and communications lawyer with the Washington, D.C.-based law firm Hogan & Harston L.L.P., first divulged evidence of the Carnivore system's abilities during a congressional hearing in April. The FBI must have a court order to use Carnivore.

Once approved, Carnivore is attached directly to an ISP's network and gives the FBI access to all e-mail traffic flowing across the network, according to the ACLU. The ACLU and others have raised concerns that Carnivore intercepts information from the headers of e-mail messages and may divulge details about the contents of the messages.

"The FBI and the law enforcement and national security communities in general are offering a trade: less privacy due to increased use of technology in surveillance in return for greater safety for the public," said Daniel Ryan, a lawyer and former director of Information Systems Security at the Pentagon. ■

Intell turf battles rage

BY DAN VERTON

Major portions of a bill that would authorize appropriations for the U.S. intelligence community would significantly limit the Defense Department's ability to support military operations, warn Defense Secretary William Cohen and his top military adviser.

William Cohen, Secretary of Defense

Cohen and Army Gen. Henry Shelton, chairman of the Joint Chiefs of Staff, recently sent a letter to senior lawmakers on Capitol Hill protesting a proposal by the House Permanent Select Committee on Intelligence to establish an intelligence community communications architect position within the CIA. The chief architect would have broad responsibilities for the development of a worldwide telecommunications system that would serve the intelligence community, the bulk of which now resides in DOD and not the CIA.

The chief architect, supported by a 30-person staff, would be funded with $80 million in start-up money taken directly from the budgets of the Pentagon's National Reconnaissance Office, the National Security Agency and the Defense Intelligence Agency, according to the bill.

"This unilateral and independent architectural office would seriously damage, if not totally destroy, the efforts of the DOD chief information officer, who has ongoing activities with the [intelligence community] and Defense intelligence component CIOs to advance interoperability between and among intelligence producers and consumers," Cohen and Shelton told Congress. The House Armed Services Committee included Cohen and Shelton's letter in a report on the fiscal 2001 Intelligence Authorization bill, released last month.

But the Pentagon is also concerned about the impact the new office might have on DOD's efforts to orchestrate a Global Information Grid (GIG), according to the Cohen and Shelton letter. The Pentagon has been working on the GIG concept for more than a year and envisions a global network capable of delivering secure information to all users.

The GIG architecture "puts a premium on the assured and timely access by our warfighters and policy-makers to all forms of information, including intelligence," a Pentagon spokesperson said. However, "there shouldn't be separate architectures for combat functions, for support functions [or] for intelligence functions. Otherwise, we're back at the stovepiped, stand-alone systems that don't talk to one another in a timely fashion."

An official from the Pentagon's office of Command, Control, Communications and Intelligence also said that the Pentagon supports a broader GIG concept as opposed to a narrow, intelligence-only communications architecture.

"Solutions which take down the old barriers to interoperability and harness our collaborative networking and computing capabilities have the most value and are deserving of support," the official said. "Our concerns with the proposed intelligence communications architect are lessened by the extent to which that entity is free to support the broader Global Information Grid architecture in preference to a narrower, intelligence-only network."

Cohen and Shelton expressed opposition to Congress' proposal to expedite the real-world use of the Joint Intelligence Virtual Architecture tool in the intelligence community, saying it is "premature" to designate the software capability as the community standard for collaboration. The program is a next-generation digital collaboration effort headed up by Defense Intelligence Agency. Congress called for oversight of the program to be transferred from DOD to the CIA.

"We feel strongly that it would be counterproductive both to prohibit further non-JIVA technology pursuits and to remove the program from the DOD oversight that has made it the success that the committee commends," stated Cohen and Shelton.

The CIA declined to comment on the proposed legislation. ■

A WAR, NOT A BATTLE

Intelligence experts characterized the latest report on the bill from the House Armed Services Committee as little more than a tool in the struggle for control over the intelligence budget between the House and the Senate Select Committee on Intelligence, chaired by Sen. Richard Shelby (R-Ala.).

Others said the debate centers on the larger questions of reforming the intelligence community and who should be in charge.

"It's just one more instance of the turf battle over intelligence," said Steven Aftergood, an intelligence specialist with the Federation of American Scientists.

"The basic question is, will there be a strong director of central intelligence who is in charge of the whole community? The Defense Department says no."

Furthermore, "because of the ongoing militarization of intelligence, my bet is that the Pentagon will get its way," he said.

Robert Steele, a 25-year veteran of the intelligence community and author of the recent book "On Intelligence: Spies and Secrecy in an Open World," said the Information Age has challenged the whole notion of having a central agency responsible for intelligence. "In the age of distributed information, the concept of central intelligence is an oxymoron," Steele said.

— Dan Verton

PHOTO/AP

Tuesday July 11 7:26 PM ET

FBI e-mail Snooping Device Attacked

By D. IAN HOPPER, Associated Press Writer

WASHINGTON (AP) - Civil liberties and privacy groups railed Tuesday against a new system designed to allow law enforcement agents to intercept and analyze huge amounts of e-mail in connection with an investigation.

The system, called ''Carnivore,'' was first hinted at on April 6 in testimony to a House subcommittee. Now the FBI has it in use.

When Carnivore is placed at an Internet Service Provider, it scans all incoming and outgoing e-mails f messages associated with the target of a criminal probe.

In a letter addressed to two members of the House subcommittee that deals with Fourth Amendment search-and-seizure issues, the American Civil Liberties Union argued that the system breaches the Internet provider's rights and the rights of all its customers by reading both sender and recipient addresses, as well as subject lines of e-mails, to decide whether to make a copy of the entire message.

Further, while the system is plugged into the Internet provider's systems, it is controlled solely by the law enforcement agency. In a traditional wiretap, the tap is physically placed and maintained by the telephone company.

''Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers, with the 'assurance' that the FBI will record only conversations the specified target,'' read the letter. ''This 'trust us, we are the government' approach is the antithesis o the procedures required under our wiretapping laws.''

Barry Steinhardt, associate director of the ACLU, said citizens shouldn't trust that such a sweeping dat tap will only be used against criminal suspects. And even then, he said, the data mined by Carnivore, particularly subject lines, is already intrusive.

''Law enforcement should be prohibited from installing any device that allows them to intercept communications from persons other than the target,'' Steinhardt said in an interview. ''When conductin these kinds of investigations, the information should be restricted to only addressing information.''

A spokeswoman for Rep. Charles T. Canady, R-Fla., who heads the Constitution subcommittee, said that the congressman had no immediate comment on the letter.

In testimony to Canady's subcommittee, Robert Corn-Revere, a lawyer at the Hogan & Hartson law fir in Washington, said that he represented an Internet provider that refused to install the Carnivore syste The provider was placed in an ``awkward position,'' Corn-Revere said, because the company feared sui from customers unhappy with the government looking in to all the e-mail.

``It was acknowledged (by the government) that Carnivore would enable remote access to the ISP's network and would be under the exclusive control of government agents,'' Corn-Revere said.

Corn-Revere told the committee that current law is insufficient to deal with Carnivore's potential and that the Internet provider lost their court battle in part because of the Internet's connection to telephone lines, and that the law was stretched to cover the Internet as well.

Corn-Revere would not reveal the name of his client, and the client lost the case. He said that the FBI has been using Carnivore since early this year.

James X. Dempsey, senior staff counsel at the Center for Democracy and Technology, said that the main problem with Carnivore is it's mystery.

``The FBI is placing a black box inside the computer network of an ISP,'' Dempsey said. ``Not even th ISP knows exactly what that gizmo is doing.''

But Dempsey said that Internet providers contributed to the problem, by saying that current technolog does not allow the Internet provider to sort out exactly what the government is entitled to get under a search warrant. The carriers complained that they had to give everything to the FBI.

``The service providers said they didn't know how to comply with court orders,'' Dempsey said. ``By taking that position, they have hurt themselves, putting themselves into a box.''

Marcus Thomas, who heads the FBI's Cyber Technology Section, told the Wall Street Journal that the bureau has about 20 Carnivore systems, which are PCs with proprietary software. He said Carnivore meets current wiretapping laws, but is designed to keep up with the Internet.

``This is just a specialized sniffer,'' Thomas told the Journal, which first reported details about Carnivore.

Encrypted e-mail, done with an e-mail encoding program like PGP, still stays in code on Carnivore, an it's up to agents to decode it.

Dempsey has a possible solution to the problem, though one that's probably unlikely - show everyone what it does and how it does it, allowing Internet providers to install the software themselves.

``The FBI should make this gizmo an open-source product,'' he said. ``Then the secret is gone.''

On the Net: Federal Bureau of Investigation: http://www.fbi.gov

American Civil Liberties Union: http://www.aclu.org

Center for Democracy and Technology: http://www.cdt.org

Pretty Good Privacy (PGP): www.pgp.com

Email this story - (View most popular) | Printer-friendly format

Archived Stories by Date: Jul 11 Go

Search News

Search Advanced

Search: Stories Photos Full Coverage

Home Top Stories Business Tech Politics World Local Entertainment Sports Science Health Full Coverag

Questions or Comments

FBI FACSIMILE

COVER SHEET

PRECEDENCE

- ☐ Immediate
- ☐ Priority
- ☒ Routine

CLASSIFICATION

- ☐ Top Secret
- ☐ Secret
- ☐ Confidential
- ☐ Sensitive
- ☐ Unclassified

Time Transmitted: _____
Sender's Initials: _____
Number of Pages: _____
(including cover sheet)

To: _____ Date: 7/12/00
Name of Office

Facsimile Number: 703-632-6081

Attn: MARCUS Thomas
Name Room Telephone

From: CIS
Name of Office

Subject: _____

Special Handling Instructions: _____

Originator's Name: [redacted] Telephone: 6C-1 / 67C-1

Originator's Facsimile Number: _____

Approved: _____

Brief Description of Communication Faxed: FYI.

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or the local FBI Office immediately to arrange for proper disposition.

Doc #17

Reno to review the FBI's Internet wiretap system

WASHINGTON, July 13 (Reuters) - U.S. Attorney General Janet Reno said on Thursday she would review a new FBI automated computer system that can wiretap the Internet to determine whether it might infringe on privacy rights.

``I'm taking a look at it now to make sure that we balance the rights of all Americans with the technology of today," Reno said when asked about the FBI system known as ``Carnivore" that can be used to monitor all e-mails of a criminal suspect.

Reno emphasised that any such wiretaps, which are placed on an Internet service provider's system, cannot be be done without an appropriate court order ``according to processes and procedures used now for lawful surveillance."

``We are looking at it to see what is needed, if anything," she said. ``If additional regulations are needed, we will pursue those."

She told her weekly news briefing that she wanted to make sure that the new technology does not become ``a cause of concern for privacy interests."

The American Civil Liberties Union (ACLU) and other privacy advocates have expressed concern the new system could scan private information about legal activities, resulting in excessive monitoring of online communications. Besides e-mails, the system can monitor visits to Web sites and Internet chat sessions.

Reno said she only began looking into the issue and asking questions after news articles appeared earlier this week. The FBI recently demonstrated the system to executives in the telecommunications industry.

``We have known about the capacity to do this. Its application and what has been done had not been brought to my attention," Reno said.

The FBI's director, Louis Freeh, reports to Reno.

``I just want to make sure that industry, privacy interests, law enforcement interests are all fully advised so that we can consider anybody's concerns and make sure that we address them," Reno said.

She was unable to say whether the system would continue to operate until her review was underway.

13:29 07-13-00

Doc. #18

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

3 Pages were not considered for release as they are duplicative of DOC. #12, OGC/TECHNOLOGY LAW UNIT FILE

_____ Page(s) withheld for the following reason(s): (PAGES 268-270)

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #19 (Pages 647-649)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Controls on Export of Encryption Software to be Eased

By John Schwartz
Washington Post Staff Writer
Monday, July 17, 2000; 1:12 PM

The Clinton administration announced today that it will loosen controls on the export of encryption software -- the programs that help users scramble messages and data to protect it from prying eyes -- and called for new legislation intended to make sense of wiretapping in the internet age.

"We need to seek a better balance amongst the sometimes competing goals of the protection of public safety, the achievement of economic growth and digital opportunity -- and the preservation of privacy and civil liberties," said White House Chief of Staff John Podesta in a speech delivered today at the National Press Club.

Under the new policy, American companies will be able to export the strongest cryptography products to users in any nation in the European Union and to Australia, Norway, the Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. The government will eliminate a current statutory 30-day waiting period before such exports can take place, but keeps in place a requirement that new technologies be submitted to the government for a technical review.

Encryption has been a high-tech battlefield from the early days of the Clinton administration. Few technologies are as important in the fight to maintain personal and business privacy -- but few technologies, as well, present such daunting issues for law enforcement, which warns that criminals and terrorists can use "crypto" to cloak their plans and activities. But high-tech companies successfully argued that U.S. restrictions only harmed American companies, since overseas firms were successfully marketing strong encryption products, and in January the Clinton administration reduced controls on encryption exports. In

the Clinton administration relaxed controls on encryption exports. In today's speech, Podesta stressed the now-familiar theme that the online revolution has been a mixed blessing. At the same time that the Internet makes Shakespearean sonnets and new photos of Mars available anywhere in the world, it has undermined the pirvacy of our most sensitive financial and medical records, and allows such evildoers as international drug trafffickers to communicate freely and secretly.

"That's why we have to make sure the Internet is used to the benefit of people – not to their detriment," the Podesta said.

The most sweeping part of the Podesta address was a call for a thorough rethinking of the Fourth Amendment's protection against unreasonable search and seizure in the Internet age. Electronic mail transmitted by high-speed connections such as DSL modems, Podesta's speech argued, has never enjoyed the legal protections the law gives to telephone conversations – or to slower dial-up modems under the Electronic Privacy Communications Act of 1984. At the same time, cable privacy laws are tougher than wiretap standards when it comes to gaining access to subscriber records – which could include e-mail sent via cable modem. Podesta called for new legislation to address the inconsistencies in the legal framework. "It's time to adopt legislative protections that map these important privacy principles onto the latest technology," he said.

Podesta's speech also make oblique reference to a controversial new surveillance technology revealed last week, which is known as "Carnivore." Carnivore gives government the ability to selectively monitor Internet traffic of individuals in ways that can give law enforcement the Internet equivalent of "trap and trace" capabilities used in telephone surveillance. Unlike full-fledged wiretaps, the judicial oversight of trap and trace is slight, and the protection against abuses of the technology by law enforcement is weak. Podesta called for "greater judicial oversight of trap and trace authorities."

Podesta's speech stated that this legislation could be passed by the end of the year – an unlikely prospect in these waning days of the legislative session. "It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations," he said.

The speech also made the point that the administration's preference is for public-private partnerships to make the Internet secure against attack, but noted that Congress has not appropriated any of the $90 million President Clinton has requested for security research and cyber policing. "It's time," Podesta noted, that "they picked up the pace and provided the protections that are essential to America's cyber security.,"

The speech was not well received by civil liberties advocates, who have fought Carnivore and other administration attempts to develop wiretapping capabilities on the Internet. Barry Steinhardt, associate director of the American Civil Liberties Union, called the speech

"deeply disappointing."

Rather than defending Carnivore, Steinhardt said, Podesta should have announced that the administration was suspending its use. "Carnivore represents a grave threat to the privacy of all Americans by giving law enforcement agencies unsupervised access to a nearly unlimited amount of communications traffic," Steinhardt said in a statement.

"While the Clinton administration's proposals have some heartening qualities to them, they are too little and too late," with too little time in the legislative session to pass new bills. "Last-minute legislative proposals cannot satisfy the deep privacy concerns of the American public," Steinhardt said.

◂ Previous Article Back to the top Next Article ▸

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

_____ Pages were not considered for release as they are duplicative of _____

3 Page(s) withheld for the following reason(s): PREVIOUSLY RELEASED AS PART OF EC PACKET #5 (RELEASE #4)

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #21 (Pages 653-655)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

July 18, 2000

Proposal Offers Surveillance Rules for the Internet

White House Tries to Balance Rights of Computer Users and Law Enforcement

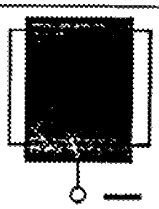
By STEPHEN LABATON with MATT RICHTEL

WASHINGTON, July 17 -- The White House said today that it would propose legislation to set legal requirements for surveillance in cyberspace by law enforcement authorities similar in some ways to those for telephone wiretaps.

Privacy advocates and civil liberties groups welcomed some aspects of the proposal but said they remained alarmed about a new F.B.I. computer system that searches and intercepts private e-mail and can easily capture communications of people not suspected of crimes.

The legislative proposal was made as the administration also announced today that it had eased export controls on encryption technology, making it significantly easier for American companies to sell software products to the European Union and eight other trading partners that can be used to keep computer data and communications secure.

Both the electronic surveillance proposal and the export control changes are part of a broader policy outlined in a speech today by John D. Podesta, the White House chief of staff. He said the policy tries to balance the privacy rights of computer users against the needs of law enforcement to be able to monitor digital communications.



NET PRIVACY

IN DEPTH
Privacy and the Internet

RECENT NEWS
Administration Retools Rules on Encryption (July 18, 2000)

Reno Says Review Is Under Way on Net 'Wiretapping' (July 14, 2000)

Administration Issues Privacy Directives (June 13, 2000)

FORUM
Can Privacy be Protected Online?

Congress and federal regulators have done little work in the area, even as the world has quickly come to rely heavily on communications through cyberspace. More than 1.4 billion e-mail messages change hands every day.

The administration's legislative proposal on electronic surveillance tries to fix the inconsistent patchwork of laws that apply different standards to telephone, cable and other technologies with a single standard for those systems and the Internet. Prospects for the proposal in Congress are uncertain.

Until now, law enforcement agencies have been able to monitor electronic communication with only modest court supervision.

The proposed legislation would require that the same standards that apply to the interception of the content of telephone calls apply to the interception of e-mail messages. Specifically, it would require law enforcement agents to demonstrate that they have probable cause of a crime to obtain a court order seeking the contents of a suspect's e-mail messages.

The proposal would also give federal magistrates greater authority to review requests by law enforcement authorities for so-called pen registers -- lists of the phone numbers called from a particular location and the time of the calls. The magistrates now have no authority to question the request for such lists, which are frequently used by the authorities.

In the context of the Internet, existing laws are ambiguous about what standards apply for different kinds of surveillance. Many limitations imposed on law enforcement in the context of telephone wiretaps -- like the requirement that such taps be approved at the highest level of the Justice Department -- do not appear to apply to e-mail surveillance.

Moreover, the Cable Act of 1984 sets a far harder burden for government agents to satisfy when trying to monitor computers using cable modems than when monitoring telephones. That has proved troublesome for law enforcement authorities as more Americans begin to use high-speed Internet service through cable networks. The Cable Act also requires that the target of the surveillance be given notice and an opportunity to challenge the request.

"It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations," Mr. Podesta said in a speech at the National Press Club. "Our proposed legislation would harmonize the legal standards that apply to law enforcement's access to e-mails, telephone calls and cable services."

White House officials said today that they hoped the proposal would break a logjam in Congress where a variety of different measures have been introduced dealing with electronic surveillance. The

administration's proposal adopts some elements of both Democratic and Republican bills.

But Congressional aides said there was too little time left in the legislative session and that the matter would in all likelihood remain unresolved until after the next term begins, in 2001.

Administration officials said the proposal would apply to communications that either begin or end in the United States. It would not apply to e-mail messages transmitted entirely outside the country.

Privacy and civil liberties groups criticized the administration's proposal because it would continue to permit the government to use a new surveillance system that the groups say may be used far more broadly than older technologies, enabling federal agents to monitor an unlimited amount of innocent communications, including those of people who are not targets of criminal investigations.

The system, used by the Federal Bureau of Investigation, is called Carnivore, so named, agents say, because it is able to quickly get the "meat" in huge quantities of e-mail messages, so-called instant messaging and other communications between computers.

Carnivore is housed in a small black box and consists of hardware and software that trolls for information after being connected to the network of an Internet service provider. Once installed, it has the ability to monitor all of the e-mail on a network, from the list of what mail is sent to the actual content of the communications.

Marcus C. Thomas, section chief of the Cyber Technology Section of the F.B.I., said the technology was developed 18 months ago by F.B.I. engineers and has been used fewer than 25 times. Mr. Thomas said that Carnivore had potentially broad capabilities and that he understood the concerns of privacy groups.

"It can do a ton of things," he said. "That's why it's illegal to do so without a clear order from the court."

He said that most Internet service providers had cooperated with requests to use Carnivore.

Privacy groups and some Internet service providers have been deeply critical of the use of Carnivore because, once installed on a network, it permits the government to take whatever information it wants.

Moreover, the government has not said what it does with the extraneous material it gathers that is not relevant to the particular surveillance.

The issue does not often arise today with the monitoring of telephone conversations because when a law enforcement authority wants to see a list of telephone calls made by a suspect, the agent

gets an order from a magistrate, presents the order to a telephone company, and the company then turns over the list.

In at least one instance, an Internet company did not cooperate so readily with the government. In December, federal marshals approached the company with a court order permitting them to deploy a device to register time, date and source information involving e-mail messages sent to and from a specified account.

Trying to establish a single standard for different technologies.

Concerned the device would record broader information, the company countered with a compromise: it would provide the government with the requested information about e-mail senders and recipients, according to Robert Corn-Revere, a lawyer for the company, in recent Congressional testimony. The company was later identified as EarthLink, a service provider with 3.5 million subscribers.

Mr. Corn-Revere said the government initially accepted the compromise but later became dissatisfied and wished to use its own device. EarthLink objected but was overruled by a a federal court, which ordered the device deployed.

Other Internet companies have also been critical of Carnivore.

William L. Schrader, chairman and chief executive of PSINet, a major commercial Internet service provider, said that the system gave the F.B.I. the ability to monitor e-mail messages of every person on a given network. He said he would refuse to permit the government to use the technology at PSINet unless agents could prove that it could only sift out the traffic from a given individual that is the target of a court order.

"I object to American citizens and any citizens of the world always being subject to someone monitoring their e-mail," said Mr. Schrader, whose company serves about 100,000 businesses and more than 10 million users. "I believe it's unconstitutional and I'll wait for the Supreme Court to force me to do it."

Civil liberties groups, meanwhile, said that today's policy announcement was an inadequate response to the growing controversy over the deployment of Carnivore.

"Today's speech was camouflage to cover the mess that is Carnivore," said Barry Steinhardt, an associate director of the American Civil Liberties Union. "In light of the public and Congressional criticism of Carnivore, we had hoped and expected far more from an administration that likes to tout its sensitivity to privacy rights. Rather than glossing over Carnivore, Podesta should have announced that the administration was suspending its use."

Facing growing concerns about

Concern that the proposals allow federal agents too much leeway.

Facing growing concerns about Carnivore, Attorney General Janet Reno said on Thursday that she would review whether the system was being used in a manner consistent with privacy rights in the Constitution and in federal law. A subcommittee of the House is set to hold a hearing next week on the system.

While the civil liberties and privacy groups applauded giving judges greater discretion to review certain kinds of requests for surveillance, they were critical of other aspects of the proposal.

Marc Rotenberg, director of the Electronic Privacy Information Center, a research organization that studies privacy issues and technology, criticized the administration for lowering the standards for surveillance of cable modems rather than raising the standards for telephone surveillance.

"The Cable Act provides for one of the best privacy protections in the United States," Mr. Rotenberg said. "The question is whether to harmonize up or harmonize down. Our view is this harmonizes down."

But administration officials said the Cable Act never contemplated that there would be broad use of cable modems for e-mail traffic and that the standards used for obtaining warrants for telephone surveillance should also apply to digital communications through cable networks.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of DOC. #10, OGC FRONT OFFICE FILE (PGS. 16 + 17)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages: DOCUMENT #23 (Pages 661-662)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

July 21, 2000, Friday 01:27 PM Eastern Time

SECTION: GENERAL NEWS

LENGTH: 713 words

HEADLINE: The FBI's **Carnivore:** It bites only under court order

BYLINE: By MICHAEL KIRKLAND

DATELINE: WASHINGTON, July 21

BODY:
The FBI is in a full-court press to reassure the public about its **Carnivore** intercept system, designed to perform a "wire-tapping" function on the Internet.

During a background briefing for reporters Friday, FBI officials said the system can only be used under court order, and that "procedure, training and audits" of its use will prevent technicians from attempting unauthorized snooping.

A senior official added that the bureau is looking for "a couple of technical institutions" outside the FBI to independently "validate and evaluate" the system's operation and integrity.

The system has drawn fire from an unlikely coalition of critics.

The American Civil Liberties Union and similar groups have attacked **Carnivore** as new government intrusion without proper safeguards. The Republican leadership of Congress has also been highly critical, and a House Judiciary subcommittee has planned hearings Monday to explore what some politicians believe is a need for new federal restrictions on its use.

Meanwhile, the average computer user may feel that Big Brother is looking over his or her shoulder.

Not so, says the FBI in its most soothing official voice.

At Friday's briefing in a conference room at bureau headquarters in Washington, the senior FBI official said the **Carnivore** program is three years old, and, "It began because we were receiving court orders to do intercepts on the Internet."

Carnivore software - so named because it looks for the "meat" in a data stream - uses a Windows platform and is contained on a personal computer that is plugged into an Internet service provider. The access is allowed only for the length of time set out in a court order. "When the order expires, we take our equipment away," the senior official said.

The ISP usually performs some "pre-filtering" of data so that the amount of information traveling through the **Carnivore** "filter" is not overwhelming. The **Carnivore** device can perform a traditional "pen register" function on the Internet - record and store the origin and destination of e-mail - or capture the content of an e-mail message, much like a traditional phone tap, only in a much more specific way.

"That filter is configured to fit the contour of the court order we're assigned to do," the senior official said. In other words, it will only select and copy specific information authorized by a federal judge. The system targets e-mail by an "authorization" code peculiar to an individual user, and the FBI will not monitor subject lines on e-mail.

The filtering process will not slow down computer response time, another FBI official familiar with the technology said. "It's just passively watching the bits."

The approval process for a **Carnivore** intercept is also extremely rigorous, an FBI official expert in cyber legal issues said. Investigators seeking a court order to use **Carnivore** must go through an internal FBI review process, then the request must be approved by the attorney general or the deputy attorney general before a federal judge is approached for a court order.

Less than a dozen such requests have been made over the last year for criminal probes - as opposed to national security investigations - and no request has been refused by a judge.

"These (intercepts) are not implemented trivially," the FBI legal official said, both because of the expense and the depth of review.

What about someone outside the FBI hacking into the **Carnivore** device and accessing an innocent person's e-mail?

"The device cannot be penetrated from the Internet side," the FBI technical official said. "Theoretically," a hacker could beat very high odds and randomly dial into a separate monitoring line, he added, but even that line is protected by heavy security.

The senior official at Friday's briefing conceded that the name of the system - **Carnivore** - has caused some apprehension. "Naming is always a very sensitive thing," the official said. "This experience is sobering." The official said the FBI would give some thought in the future to the effect the name of an operation or procedure might have on the public.

"Sniffer" might be a fairer term. "It's a customized packet sniffer," the FBI technical official said.

"A very well-focused sniffer," the senior official added.

LANGUAGE: ENGLISH

LOAD-DATE: July 21, 2000

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

10 Pages were not considered for release as they are duplicative of DOC. #13, OGC FRONT OFFICE FILE, PGS 16-25

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #25 (Pages 665 - 674)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

5 Pages were not considered for release as they are duplicative of DOC. #20, OPCA FILE (PGS. 514-518)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #26 (Pages 675-679)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

The Feds Can Read Your E-Mail

NewsMax.com
Wednesday, July 12, 2000

First it was Echelon, the global eavesdropping system Uncle Sam and John Bull have been using to spy on satellite-transmitted phone calls, e-mails and fax messages. Now it's Carnivore, the FBI's newest electronic snooping device that can read your e-mail right off your mail server.

Capable of scanning millions of e-mails a second, Carnivore can easily be used to monitor everybody's e-mail messages and transactions, including banking and Internet commerce. If they want to, the feds can find out what books you're buying online, what kind of banking transactions you conduct – in short, everything you do when you go online and send e-mail, whether private or commercial.

The FBI has been quietly monitoring e-mail for about a year. Two weeks ago the feds went public and explained the high-tech snooping operation to what the Wall Street Journal called "a roomful of astonished industry specialists."

According to the bureau, they've used Carnivore – so called because it can digest the "meat" of the information they're looking for – in less than 100 cases, in most cases to locate hackers but also to track terrorist and narcotics activities.

But there is nothing to stop Carnivore from making a meal of your e-mail messages and transactions if they decide that's what they want to do and can get a judge to issue a court order allowing them to tap your e-mail as they would your phones.

That's scant comfort considering the underhanded means the feds employed to get court orders to raid the Branch Davidian compound, or to win a judge's permission to stage what amounted to an illegal armed raid on Elian Gonzalez's Miami home.

Carnivore is nothing but a store-bought personal computer with special software that the FBI installs in the offices of Internet service providers (ISPs).

The computer is kept in a locked cage for about a month and a half. Every day

an agent comes by and retrieves the previous day's e-mail sent to or by someone suspected of a crime.

But critics say that Carnivore, like some ravening beast, is simply too hungry to be trusted – that it gives the feds far too much access to too much private information.

"This is more of a vacuum cleaner-type approach – it apparently rifles through everything," David Sobel, general counsel for the Electronic Privacy Information Center, told Fox News.

"It's potentially much more invasive than telephone surveillance."

Carnivore could conceivably monitor all the e-mail that moves through an ISP – not merely messages sent to or from the subject allegedly being monitored. Critics compare it to eavesdropping on all the phones in a neighborhood simply to zero in on just one phone.

Disturbingly, the FBI has prevailed in challenges against forcing ISPs to allow Carnivore to be installed in their offices. According to the Wall Street Journal, one unidentified ISP put up a legal fight against Carnivore early this year and lost.

The FBI defends Carnivore, insisting it is used selectively and monitors only the e-mail of the subject. They say that messages belonging to those not being probed, even if criminal, would not be admissible in court.

"The volume of e-mail in a location is generally fairly small and being managed by a small number of e-mail servers on a fairly low-speed network," said Marcus Thomas, chief of the FBI's cyber technology section.

"The system is not unlike 'sniffers' used within the networks every day."

That fails to satisfy critics such as Sobel. He says Carnivore is similar to Russia's surveillance system, called "SORM," which all Russian ISPs are forced to install to allow the government to spy on whomever it chooses.

It's also similar, he says, to the notorious Echelon, the National Security Agency's global eavesdropping system, which intercepts telecommunications transmissions from around the world and looks for keywords that could indicate illegal activity.

"Carnivore is really the latest indication of a very aggressive stance that the bureau is taking in collecting as much information as technically possible," Sobel said.

FBI spokesman Paul Bresson insists that law-abiding citizens have nothing to fear from Carnivore. "Anytime we develop a system, we're basically balancing the interests of national security against that of the privacy of the public," he said.

"This issue's always going to come up. We're always going to get questions. We understand that."

See articles on Echelon.

E-mail This Article to a Friend

Printer Friendly Version

E-mail a Comment to NewsMax.com Discuss this Article in NewsMax.com's Forum

Reprint Information

Home · Search · Free E-mail News · ZipMax.com-Free Webmail · Columnists · News Links · Late Night Jokes

Archives · Shopping Mall · Cartoons · Magazines · Forum · Classifieds · Contact Us

FBI FACSIMILE

COVER SHEET

Ed Marcus

PRECEDENCE

- ☐ Immediate
- ☐ Priority
- ☒ Routine

CLASSIFICATION

- ☐ Top Secret
- ☐ Secret
- ☐ Confidential
- ☐ Sensitive
- ☒ Unclassified

Time Transmitted: 3:30 pm
Sender's Initials: slk
Number of Pages: 4
(including cover sheet)

To: Ed Allen
Name of Office

Date: 07/26/2000

Facsimile Number: 703-632-6081

Attn: _____
Name Room Telephone

From: FBI - San Diego
Name of Office

Subject: _____

Special Handling Instructions: _____

Originator's Name: SAC William D. Gore Telephone: 858-514-5600

Originator's Facsimile Number: 858-514-5890

Approved: WDG

Brief Description of Communication Faxed: _____

WARNING

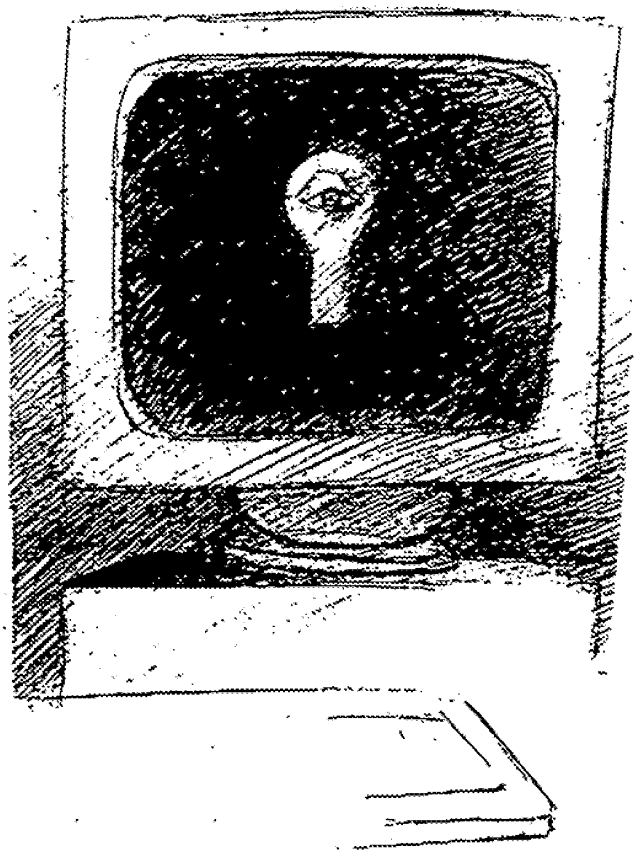
Doc #28

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or the local FBI Office immediately to arrange for proper disposition.

FD-350 (REV. 5-8-81)

MOUNT CLIPPING IN SPACE BELOW

The Eye of the FBI



Paul Tong

Indicate page, newspaper, city, state
San Diego Union Tribune
San Diego, California

Page B-9

July 26, 2000

Title:
"The Eye of the FBI"

Submitting Office:
San Diego

Indexing:

"Eye of the FBI" (continued)

By Lisa S. Dean

For those of you who thought that ECHELON, the multinational surveillance system, was a joke, here's something else for you to laugh at. It's a new system called "Carnivore" operated by the Federal Bureau of Investigation.

The aptly named system is placed at the Internet service provider level and monitors online communications looking for criminal activity. That may not sound too bad because the FBI claims to actually be looking for criminals, and let's assume for the sake of argument that it is.

There are still two problems with "Carnivore." First, instead of having a warrant to, in effect, tap an Internet user's account for suspected illegal activity, "Carnivore" just taps everyone's communications and like ECHELON, filters them to look for illegal activity. As a result, your private e-mails to your friends and family perhaps discussing very personal family matters, will end up in the hands of the FBI.

This leads to the second problem, namely a clear violation of the Fourth Amendment which is supposed to protect us from such activities performed by the government. Let me remind you of the wording of the Fourth Amendment: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The FBI's "Carnivore" system completely disregards that amendment because of its broad-sweeping powers to intercept hundreds of thousands of messages at one time from innocent citizens. How does one obtain a warrant to tap hundreds of thousands of e-mail addresses at one time? Moreover, unless a government treats all of its citizens as guilty until proven innocent rather than the reverse, there is no "probable cause" to intercept the enormous amount of e-mail communications, and that too is a violation of the Fourth Amendment.

Since we're talking about cyberspace here, law enforcement is going to have a tough time "describing the place to be searched and the persons or things being seized." Also, since we're talking about cyberspace where evidence is intangible rather than tangible, it would facilitate law enforcement's ability to seize property from one's computer without a warrant.

If you think that would never happen, just look at the recent bill in both houses entitled "The Methamphetamine Anti-Proliferation Act," which gives law enforcement the ability to enter your home or tap your online communications and seize property both on and off-line without your knowledge.

But again, law enforcement has to obtain a warrant to even monitor your online conversations, right? Right, but we have observed over time the ease with which law enforcement obtains warrants to perform wiretaps.

Very few are refused by judges. In fact, it's almost a guarantee

---

Dean is vice president for technology policy at the Free Congress Foundation.

"Eye of the FBI" (continued)

to law enforcement that their requests for warrants will be granted. Since 1968 when Congress passed the wiretap law, 28 requests have been denied out of a total in excess of 20,000. In 1996, one request was denied, the first since 1988. This illustrates a lack of oversight with regard to wiretapping on the part of Congress.

But would a respectable agency such as the FBI really stoop to these sorts of practices? The evidence suggests it has done so already. In addition, in Senate testimony FBI Director Louis Freeh has said, "We need a Fourth Amendment for the Information Age." So, clearly, this agency has little regard for the wording of the one given to us by our Founders because the original amendment would forbid such systems as "Carnivore" and some other questionable surveillance practices conducted by the agency.

Where does the FBI get its authority to conduct these practices? In 1986 Congress passed the "Electronic Communications Privacy Act" to update the federal wiretap law enacted in 1968 by including new communication technologies, such as wireless and electronic communications, under jurisdiction of the existing law.

Then in 1994, Congress, in an attempt to update the law, passed the Communication Assistance for Law Enforcement Act, or CALEA, which essentially told the telecommunications carriers that as its technology developed, it had to design its systems in such a way that it did not impede the ability of law enforcement to conduct wiretap surveillance. CALEA was not to be interpreted as expanding the authority of law enforcement in the area of wiretap surveillance. Very simple.

Immediately after the passage of CALEA, the FBI interpreted the law beyond the boundaries for which it was intended, namely, to include location tracking of cell phone users and "roving wiretaps," allowing law enforcement to obtain a warrant to tap all of the phones within the vicinity of a suspect rather than the traditional practice of tapping a suspect's own telephone line.

The agency also gave itself the authority to design the telecommunications systems throughout the United States. The agency then wanted to further interpret the law to include wiretapping online communications such as e-mail but was refused the authority to do so.

Now comes "Carnivore" which does exactly what the FBI wanted in the first place. Aside from the gross expansion of snooping capability into every computer user's online correspondence, "Carnivore" provides the agency with the ability to carry out procedures which it legally cannot perform, namely the ability to order an ISP to turn over all of the e-mail addresses of users who correspond with a particular suspect or to gain access to the list of an ISP's subscribers.

The boldness and brashness of this federal agency is astounding. While Congress is debating such measures as Social Security or tax reform, issues that it has been haggling over since the Reagan era, it needs to pause and take a sharp look into this agency's practices.

The "Carnivore" system is perfectly named because it is devouring our liberties faster than we can protect them. If we don't start looking into matters such as this which are related to our liberties, congressional debates over education or welfare reform won't make a difference to the future of our nation.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

76 Pages were not considered for release as they are duplicative of DOC #14 OGC FRONT OFFICE FILE (PAGES 45-120)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages: DOCUMENT #29 (Pages 687-762)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

CARNIVORE

(Vol. 67, No. 16)

News

Electronic Surveillance

Existing Laws Permit Collection Of Information From E-Mail, FBI Says

The Federal Bureau of Investigation takes the position that current federal law gives it the authority to implement the use of special software and hardware called "Carnivore" to collect information from the e-mail messages traveling through an Internet service provider's e-mail server, according to testimony by FBI and Justice Department officials July 24 at a congressional hearing. The hearing before the House Judiciary Committee's Subcommittee on the Constitution was convened in response to an uproar triggered by a July 11 article in the *Wall Street Journal* disclosing the existence of Carnivore.

According to the officials' testimony, if an Internet service provider is financially or technologically unable or unwilling to provide information on e-mails pursuant to a court order, the FBI will hook a Carnivore unit up to the ISP's server. Carnivore scans what officials refer to as "the smallest subset" of information from incoming and outgoing e-mail messages. Carnivore then duplicates the information and lets the transmission stream continue to flow.

Carnivore reads the incoming information and filters it according to protocols based on the original court order. Usually, the order will authorize the FBI to collect the "to" and "from" information from messages going to and from a particular e-mail address. Only the relevant information will be recorded. All extraneous information will remain only temporarily in the random access memory and will not be fixed in a stable, recorded format.

The result, according to the FBI, will be a list of e-mail messages that have been sent from or received by a particular e-mail address along with the "to" and "from" information. The FBI likens this to the results obtained by a combination of telephone trap-and-trace and pen register devices, which produce a list of telephone calls to and from a particular number giving only the calling number or the number called.

The FBI has implemented Carnivore 16 times since January and about 25 times overall since it was put into operation two years ago, according to Donald M. Kerr, assistant director of the FBI.

Current Law Authorizes Carnivore. Kevin V. di Gregory, deputy assistant attorney general for the criminal division, testified that the FBI is authorized to implement Carnivore by the current pen register and trap-and-trace law, 18 USC 3121 et seq., and wiretap law, 18 USC 2510-22.

The pen register law allows an FBI investigator to apply for an ex parte order from a court by submitting an affidavit affirming a certification by the applicant that "the information likely to be obtained is relevant to an ongoing criminal investigation." The investigator need not make a showing of probable cause, and the court does not have the discretion to refuse to issue the order.

By following this procedure, the FBI may also obtain from an ISP the "to" and "from" information from incoming and outgoing e-mail messages for a particular address.

Rep. Jerrold Nadler (D-N.Y.) expressed concern that a subject of such scrutiny might never come to know that his privacy had been invaded in such a manner, because the pen register law does not require disclosure if no charges are ever brought.

Di Gregory disputed that any invasion of privacy would have taken place in such a situation. He said that U.S. Supreme Court precedents establishing that a telephone user has no legitimate expectation of privacy in the numbers he dials supports the view that an e-mail user has no such expectation of privacy in the addresses on incoming and outgoing e-mail communications.

According to di Gregory, the FBI may gain access to the content of e-mail messages under the wiretap law. The wiretap law requires a high-ranking officer of the Justice Department to authorize an application for a court order. The court may then issue an order authorizing the government to listen in on a telephone conversation if it finds that there is probable cause to believe that someone is committing, has committed, or is about to commit one of the offenses listed in 18 USC 2516, that there is probable cause to believe that a wiretap will intercept communications concerning that offense, that normal investigative procedures have failed or appear to be unlikely to succeed or are too dangerous, and that there is probable cause to believe that the line to be tapped is the line that is likely to be used for such a communications.

According to Kerr and di Gregory, implementing Carnivore under these statutes will result in minimized and particularized information gathering, and does not amount to a search of all incoming and outgoing e-mail messages traveling through an ISP's server. Additionally, in-house, technological, judicial, and adversarial oversight will ensure that these methods are not abused.

Groups Dispute Claim of Authority. This assertion was flatly contradicted by Barry Steinhardt of the American Civil Liberties Union, who said that such filtering necessarily involves the inspection of every single e-mail message traveling through a server. Such broad authority to filter through private communications was never contemplated by Congress when passing the pen register and wiretap laws, Steinhardt said. Furthermore, he said, no matter what promises the administration makes regarding limiting its data gathering powers, recent history should warn Congress not to believe those promises.

Steinhardt offered as an example the passage of the Communications Assistance to Law Enforcement Act of

Doc. #30

1994, 47 SC 1001 et seq., which resulted from a compromise with law enforcement agencies afraid that new technology would hamper surveillance of telephone calls. He said that in exchange for requiring new digital telephone networks to be constructed to preserve existing surveillance capabilities, the FBI agreed not to use the statute to try to require telephone service providers to create new surveillance capabilities. Nevertheless, according to Steinhardt's testimony, the FBI has "consistently sought greater capacity and new surveillance features that did not exist in 1994. In some cases, they have sought capabilities that they specifically promised the Congress they would not seek."

Filtering out "to" and "from" information is not as easy as the FBI makes it sound, according to Alan Davidson of the Center for Democracy and Technology. Davidson presented the subcommittee with examples of the type of data packets that are collected by Carnivore. In many cases, he said, the "to" and "from" information that the FBI is seeking cannot be obtained without looking in the body of the message.

Both Steinhardt and Davidson, as well as Peter William Sachs, president of New Haven, Conn., ISP ICONN LLC, testified that the type of information that the FBI says it wants from Carnivore can be easily gathered by the ISPs themselves and turned over to law enforcement agencies who have obtained appropriate court orders.

Both Sides Living in the Past. Both law enforcement and civil liberties groups are still thinking in terms of the traditional switched telephone network, according to Stewart Baker, a technology expert with the Washington law firm of Steptoe & Johnson, and former general counsel to the National Security Agency.

Baker said that it is unrealistic to expect ISPs, particularly small ones, to be capable of complying with such an order on its own. "The FBI has got it right," he said. Without Carnivore or some similar program, ISPs would be faced with "an extensive unfunded mandate" to collect information pursuant to court orders.

On the other hand, for the government "to say you don't have an expectation of privacy in information held by a third party is just crazy," Baker said. "Our entire lives are in the hands of third parties."

Some kind of technological solution is necessary for law enforcement to keep up with techno-savvy criminals, he said. At the same time, innocent people must be given protections. Whatever the Congress does decide to do, it must decide quickly, Baker said, or legislation will have been mooted by technological developments.

New Legislation on Horizon. The subcommittee's hearing came a week after a White House official outlined plans by the Clinton administration to introduce a bill that would update both privacy laws and provisions through which wiretapping in all its forms is utilized. The bill, which the White House has yet to send to Congress, would regulate under what circumstances law enforcement could view, listen to and trace e-mails, cellular phone calls, and transmissions over cable networks.

Speaking at the National Press Club July 18, White House Chief of Staff John Podesta said the bill "would amend statutes using outmoded language and that are hardware-specific so that they are technologically neutral. In other words, the legislation would apply equal standards to both hardware and software surveillance."

The White House is characterizing the proposal as one that would increase privacy protections by requiring that court orders authorizing the interception of e-mail be preapproved by high level Justice Department officials. Additionally, the proposal would also make it easier to identify someone who is calling or using electronic means to contact an individual by requiring only one "trap and trace" order to trace a call or Internet session back to the source. Currently, law requires an order to be issued for each separate trace of an e-mail, which are usually bounced around by a number of different Internet services during a transmission, thus requiring multiple orders to trace a single e-mail. Any such orders must be issued by a judge after a factual finding that the standard for criminal activity was met.

The bill also allows for tracing to be conducted without prior court approval in the case of an "emergency," such as actions that threaten national defense, or large-scale hacking attempts. Such orders would be subject to judicial review within a 48-hour period. Another provision would grant authorities the same access to the Internet traffic of consumers using cable modems as those who use dial-up modems.

"With our proposal, we would retain the underlying purpose of the Cable Act to keep confidential the list of shows that customer has watched," Podesta said, "but when cable systems are used to access the Internet through cable modems, we believe the rules should be the tough but sensible standards we also support for e-mails and telephone calls."

Though the White House has no target date for sending up the legislation, the administration is confident they will be able to work with Congress to pass the legislation. "We've been able to strike the middle ground, which will enable us to get there fairly quickly," White House Spokesman Jake Siewert told BNA.

Records

DOJ Agrees to Release of Documents Underlying Report on FBI Crime Laboratory

Over 53,000 pages of background information pertaining to the Justice Department inspector general's investigation of the Federal Bureau of Investigation's crime laboratory are subject to disclosure as a result of the recent settlement of a Freedom of Information Act suit, the National Association of Criminal Defense Lawyers announced July 7. NACDL and its then-press officer, Jack King, were the original plaintiffs in the suit and were later joined by Dr. Frederic Whitehurst, a former employee of the lab whose allegations prompted the investigation.

Besides allowing the plaintiffs to disclose the documents, the settlement calls for the Justice Department to pay $355,000 in attorney's fees and to post a pointer on its website referring inquiries about the documents to NACDL's and Whitehurst's websites.

NACDL spokesman Todd Wells said the organization would make the materials available on compact disc for a cost of $40. Orders can be placed by calling (202) 872-8600.

CNN

SHOW: CNN TODAY 13:00
July 24, 2000; Monday
Transcript # 00072411V13

TYPE: LIVE REPORT
SECTION: News; Domestic
LENGTH: 301 words
HEADLINE: FBI Defends 'Carnivore' E-Mail Wiretap on Capitol Hill
BYLINE: Kyra Phillips, Pierre Thomas
HIGHLIGHT: FBI officials are on Capitol Hill today defending their new wiretap for the information age. It's called Carnivore and it's designed to selectively monitor computer e-mail to and from a suspect. It can only be used with a court order. Still, critics are concerned about possible privacy violations.

BODY:

THIS IS A RUSH TRANSCRIPT. THIS COPY MAY NOT BE IN ITS FINAL FORM AND MAY BE UPDATED.

KYRA PHILLIPS, CNN ANCHOR: FBI officials are on Capitol Hill today defending their new wiretap for the information age.

It's called Carnivore and it's designed to selectively monitor computer e-mail to and from a suspect. It can only be used with a court order. Still, critics are concerned about possible privacy violations.

More now on the controversy. Here's Justice correspondent Pierre Thomas.

Hi, Pierre.

PIERRE THOMAS, CNN JUSTICE CORRESPONDENT: Hi, Kyra. As you pointed out, the FBI says Carnivore is a new investigative tool which can tap into the e-mail of a suspect, but only with a court order. But critics say it's Big Brother on the Internet. And today, Congress wanted answers.

(BEGIN VIDEO CLIP)

UNIDENTIFIED MALE: Even a system designed with the best of intentions to legally carry out essential law enforcement functions may be a cause for concern if it's use is not properly monitored.

REP. JOHN CONYERS (D), MICHIGAN: Constitutional rights don't end where cyberspace begins.

(END VIDEO CLIP)

THOMAS: But the FBI was quick to point out the restrictions that govern Carnivore. The FBI's top lab official explained the safeguards.

(BEGIN VIDEO CLIP)

UNIDENTIFIED MALE: In every case we require a court order. That court order is specific to the numbers we target, if you will, the addresses we can target.

Doc 31

(END VIDEO CLIP)

THOMAS: Today was a fact-finding hearing and there was one point of early agreement: Carnivore may not be the best name for this system -- Kyra.

PHILLIPS: All right, Pierre Thomas, thanks so much.

LANGUAGE: ENGLISH

LOAD-DATE: July 24, 2000

COMMUNICATIONS TODAY

July 24, 2000

SECTION: Vol. 6, No. 140
LENGTH: 1097 words
HEADLINE: From the Editor's Desk... Paul Coe Clark III
BODY:
Who's Afraid Of The Big, Bad Carnivore?

This week, it finally happened: the government made clear its intent to expand wiretapping from switched voice traffic to Internet traffic. The implications for Internet-service providers and cable operators are enormous.

Last Monday, White House Chief of Staff John Podesta proposed a bill to (in my assessment) expand the voice wiretapping allowed under the Communications Assistance for Law Enforcement Act to e-mail. Podesta defended the FBI's "Carnivore" packet-sniffing software, which allows the government to read the address information and content of e-mail.

My coverage of the proposal (CT 7/18) was quite restrained, as I wanted to give it fair scrutiny before judging it.

I've given the plan that scrutiny, and I think it's a bad one. Here are two reasons why:

1) The administration avoided honest debate on the rationale for spying on citizens. Podesta, in particular, misrepresented the uses of wiretaps. He also was misleading in saying there had been no improper voice wiretaps, a "fact" he used to support IP wiretapping.

FBI and Justice Department officials, in testimony to Congress, inevitably tout wiretapping as a solution to terrorism and child pornography -- political hot-button crimes everyone opposes. That testimony draws favorable press coverage and congressional support. Who wants to be portrayed as supporting those crimes?

Podesta hit the same theme in describing Title III of the 1968 Crime Control and Safe Streets Act, which set the rules for voice wiretapping. The administration wants to apply Title III-type rules to Internet spying.

"It only allowed wiretaps in the most serious crimes, such as espionage, treason and crimes of violence," Podesta said.

But those are rarely the crimes against which law enforcement uses wiretaps. The 1999 wiretapping report by the Administrative Office of the United States Courts (available on the Web site of the Electronic Privacy Information Center) shows there were 1,350 Title III wiretaps last year. There were only 174 in 1968.

The report includes a breakdown of the crimes that were the basis for each wiretap. A full 978 of the wiretaps in 1999 were drug cases. Agencies rarely mention that fact when seek wiretapping authority, because they know it weakens their argument. Tap our phones because terrorists might blow someone up? Maybe so. Tap them because someone, somewhere, is smoking a joint? I don't know.

Drug cases were followed by racketeering (139 cases). Only when we get to homicides/assaults (62 cases) do we hit the "crimes of violence" cited by Podesta. National-security wiretaps do not even come under Title III, but the Foreign Intelligence Surveillance Act. There were 886 wiretaps under FISA in 1999. No breakdown of those cases is available, so we can't tell if they were indeed for treason and espionage. The FBI, of course, has a history of using national-security authority to wiretap such notorious menaces to the common weal as Martin Luther King Jr., John Lennon, and any reporters who happen to annoy Richard Nixon.

Doc #32

Podesta said that all wiretapping has met Title III standards. "I know of no case in which a wiretap was thrown out" for violating those standards, he said. Not yet, maybe. But the current Ramparts police scandal in Los Angeles resulted in testimony about hundreds, if not thousands, of illegal wiretaps. I asked Podesta how he could reconcile that fact with his statement. Neither he nor his aides could. They had no answer.

2) Carnivore IP wiretapping is fundamentally different from CALEA voice wiretapping. Taps on switched phone circuits, by their nature, record only the phone calls and tracing information of individual lines. Carnivore, by its nature, must intercept all traffic through an ISP to find the suspect messages. We have nothing but the government's assurances that it will ignore traffic for which it has no warrant.

Carnivore also can read content of e-mails, as well as addressing information. Under Podesta's proposal, the government standard for intercepting address information would be lower, as it is for pen-register and track-and-trace information for voice calls. A pen-register intercept, however, does not give access to the voice call. Carnivore gives access to the text of e-mails. Again, we have only the government's assurances that it will ignore the content.

Not all elements of the Podesta proposal are bad. He proposes requiring probable cause (the Title III standard) to intercept the content of e-mail. And one element, the removal of the protections against cable surveillance in the Cable Act of 1993, is inevitable. Whatever rules result from this legislation should surely apply evenly to ISPs of all technological stripes.

The depressing thing is how eagerly the phone industry now supports CALEA. The Telecom Industry Association was involved in developing the J-STD-025 wiretapping standard and Carnivore, which was unveiled late last month at the TIA-organized Joint Experts Meeting in Washington. "The FBI's program is extremely sophisticated," TIA said Tuesday. Carnivore works with Microsoft Outlook, Lotus Notes and other e-mail programs, the association continued.

Equipment vendors, who originally balked at CALEA, now consider wiretapping a profit center. ADC [ADC] just rolled out its NewNet CALEAserver wiretapping line. "It receives the intercepted communications data from various circuit-switched network elements, processes it to conform to the requirements of J-STD-025, and then distributes it to the appropriate LEA collection facilities," the company said proudly Thursday.

Comverse Infosys [CMVT] also rolled out gear this week. "Comverse Infosys is the industry leader in the legal interception market worldwide," President Dan Bodner bragged.

Current rumblings suggest ISPs are less happy about spying on their customers. Don't be fooled, though -- they'll do it. The Podesta proposal and CALEA should be stopped before spy equipment becomes an inextricable part of our basic communications network.

Paul Coe Clark III is the editor of Communications Today. He can be reached at (301) 340-7788, ext. 2037, or at pclarkfphillips.com.

LANGUAGE: ENGLISH

LOAD-DATE: July 24, 2000

CNBC News Transcripts

SHOW: RIVERA LIVE (9:00 PM ET)

July 24, 2000, Monday

LENGTH: 1375 words
HEADLINE: WHETHER THE GOVERNMENT SHOULD BE ALLOWED TO INTERCEPT INTERNET E-MAILS
ANCHORS: DAN ABRAMS
REPORTERS: JOE JOHNS
BODY:

Mr. DONALD KERR (Director, Lab Division, FBI): Hackers break into financial service company systems and steal customers' home addresses and credit card numbers. Criminals use the Internet's inexpensive and easy communications to commit large-scale fraud on victims all over the world, and terrorist bombers plan their strikes using the Internet. Investigating and deterring such wrongdoing requires tools and techniques to--designed to work with new and evolving computer and network technologies.

DAN ABRAMS, host:

But how far should law enforcement be permitted to go to combat criminals? Should they be able to tap into someone's e-mail to see what is sent out and received? The FBI says yes, and they say they now have a new surveillance system that can isolate a suspect's messages without invading the privacy of others, an electronic strainer of sorts. They say it has the same effect as a phone wiretap, a rarely used technique to monitor a specific suspect with permission from a judge. But others say the FBI's new Carnivore system, as it is known, is an invasion of privacy, that it's nearly impossible to isolate only the relevant e-mails and that the FBI would have access to far too much information. Today the debate landed on Capitol Hill. NBC's Joe Johns reports.

JOE JOHNS reporting:

Fears that e-mail from law-abidding users of the Internet could be swept up in a new FBI computer system designed to catch terrorists, con artists and hackers led Congress to schedule today's hearing. But some on Capitol Hill say drastic action may be needed to put the brakes on the FBI e-mail, wiretap system known as Carnivore.

Representative RICHARD ARMEY (Republican, Majority Leader): Well, I would shut down Carnivore now if I were at the agency.

JOHNS: Carnivore is a computer application installed on a PC that agents connect to the hardware of an Internet service provider to search for specific senders and receivers of messages. The FBI needs a court order to use it and says only targeted information is retrieved, that no indiscriminate snooping is allowed.

Mr. KERR: We're not in the, you know, broad surveillance business in any way. We're a law enforcement agency limited in what we do by what the courts order us to carry out.

JOHNS: But many Internet service providers don't like it.

Mr. CHARLES ARDAI (Juno Online Services): I think our customers would not take kindly to the idea that their private information could be available to a government agency.

JOHNS: Still one scholar who specializes in privacy issues says it's a tool law enforcement needs.

Doc. #33

Mr. AMITAI ETZIONI (George Washington University): Now more and more communications advance through the Internet. And without intercepts, we--the FBI cannot do its job.

JOHNS: Even if Congress is persuaded that Carnivore does not invade privacy, the system may still face a challenge. The American Civil Liberties Union has filed a Freedom of Information request demanding Carnivore computer codes that the government wants to keep secret. Joe Johns, NBC News, the Capitol.

ABRAMS: Joining us now from Washington is Ari Schwartz from the Center for Democracy and Technology. He's an expert on privacy and the Internet. Nancy Grace and Michael Nasatir remain with us to discuss Carnivore and cybersnooping by the feds.

Mr. Schwartz, let--let me start with you. Why is this any different, in effect, than a wiretap?

Mr. ARI SCHWARTZ (Analyst, Center for Democracy and Technology): Well, it's different in a few ways. The--the biggest difference right now is that with--with a digital wiretap, we know we have the technology--we know what is--what--what the tap--what kind of taping is going on. This system is completely closed. It's a black box that's put on to the Internet service provider. Even the Internet service provider doesn't know how it works. That's much different than the way that phone--than--than phone wiretapping happens now.

ABRAMS: Yeah. But the FBI's given these demonstrations to various people to say, 'Look, we've got a method in place. We've got a system which is going to, in effect, treat this like a phone tap. We can isolate exactly which person's e-mails we want to tap into.' And with, you know, all of the cyberterrorism, in addition to the non-cyberterrorism which is occurring through the Internet, I think a lot of people are saying, 'I'd feel a lot more comfortable if I know that my FBI can be snooping on possible terrorists.'

Mr. SCHWARTZ: Well, the--there's n--there's nothing at--we--what we need is balance, and that's really what we're getting at here, is we need a balance between privacy and--and the--the kind of searches that you're talking about. The problem that we've seen is that--the difference of showing a demo about what--what gets pulled out is different than s--than knowing the technology, knowing what's kept in the logs, what can be retrieved later on. That's much different. As I said, we have the code for--for the phone tapping system. Why can't we just see the code in this case?

ABRAMS: And--and--and what is the argu--the argument on the other side is that it's patent protected and that it would allow hackers to break into it, right?

Mr. SCHWARTZ: Well, th--that's what their--that's what their concerns are. But, of course, again, as I said, we have the same--we have the same thing set up with the digital phone network. We've had hackers in the--in the phone networks as well. You know, why can't we--we should just be able to see this code and have it open.

ABRAMS: And--and so that's your--that's your primary grip. I mean, is your--if--if...

Mr. SCHWARTZ: Well, that--that--that's the main concern with Carnivore right now. The other concern that Carnivore raises and shows for the future is the question of the decay of the Fourth Amendment. We're having a lot more information now stored on computer systems and on third-party systems than we ever have in the past. When the framers of the Constitution wrote the Fourth Amendment, which is protections from unreasonable searches and seizures by the government, people had the files in their home. The government had to come and knock on their door. That's not the case today.

ABRAMS: Nancy Grace, Fourth Amendment problem?

Ms. NANCY GRACE (Anchor, Court TV): Well, you know, of course that's not what the framers had in mine when they wrote the Constitution. But, Dan, the Fourth Amendment has been applied for everything from abortion rights to what you carry in your car trunk. It can certainly be applied to computer access. My only concern is, you know, years and years and years of Fourth Amendment law regarding wiretap has developed over the past decades, and that same law needs to be applied now to intercepting Internet communications. It cannot be a fishing spree on the part of the government. On the other hand, a warrant allows you to open doors, open boxes, open mail and open the Internet.

ABRAMS: Got to take a break. Our topic this part is Big Brother's Watching. When we come back, we're going to talk about a sheriff who is putting Web cams in his prison. We'll be back in a minute.

(Announcements)

ABRAMS: Before we get to the sheriff who has installed Web cams in his prison, I want to talk to Michael Nasatir about this issue of this FBI program that you can attach to Internet service providers to basically look at what people are e-mailing. What do you think?

Mr. MICHAEL NASATIR (Criminal Defense Attorney): You know, I think what the gentleman from Washington is saying is, 'Look, let's--let's let the civil libertarians have a crack and see what they're really going to do. It cannot be a secret. The technology has got to be--we've got to be able to study it to know what we're objecting to or not objecting to. And at the very least I do agree with Nancy Grace. Let them get a court order for--and keep it specific and have the F--Fourth Amendment apply for sure.

ABRAMS: Well--and I think there's no question that there would be--they'd have to make an application for a warrant the same way they do with a wiretap. I want to thank Ari Schwartz for joining us and talking about this topic.

LANGUAGE: English

LOAD-DATE: July 25, 2000

ABC NEWS

SHOW: WORLD NEWS THIS MORNING (6:00 AM ET)

July 24, 2000, Monday

TYPE: Newscast
LENGTH: 324 words
HEADLINE: FBI E-MAIL SURVEILLANCE PROGRAM COMES UNDER FIRE
ANCHORS: ANDERSON COOPER
REPORTERS: ANDREA McCARREN
BODY:

ANDERSON COOPER, anchor:

Federal agents say they've come up with a high-tech way to find criminals who use cyberspace to plan illegal acts, but critics contend the system, called Carnivore, simply goes too far. That is the focus of a hearing on Capitol Hill today. Here now is ABC's Andrea McCarren.

ANDREA McCARREN reporting:

(VO) The FBI says Carnivore is an essential law enforcement tool to police in the rapidly growing world of cyberspace.

Mr. DONALD KEER (Assistant Director, FBI): The range of crimes that are facilitated by computers didn't exist before, so we now have Internet fraud rather than fraud on paper.

McCARREN: (VO) The technology allows the FBI, with a court order, to sift through thousands of private e-mails selecting out those to and from a particular criminal suspect, but privacy advocates say the system is too broad because it sorts through the private e-mail of innocent people, too.

Mr. AL GIDARI (Privacy Specialist): It's a little bit like looking at all the cars on a highway just to find the blue Honda you want, and it's--it's extremely intrusive.

McCARREN: (VO) The Clinton administration proposed that the strict privacy standards that apply to telephone service be extended to electronic communications.

Mr. JOHN PODESTA (White House Chief of Staff): What we're interested in is coming up with a balance that accounts for the needs of law enforcement to pursue--pursue organized crime and narcotics traffickers but also protects the privacy of individual Americans.

McCARREN: (VO) Over the last year, the FBI has used Carnivore in about 25 criminal investigations.

(OC) Now, amid growing privacy concerns, the agency plans to submit Carnivore to a third party for an independent assessment. The FBI wants to keep secret how the technology works but, at the same time, reassure the public that their online privacy is protected. Andrea McCarren, ABC News, Washington.

LANGUAGE: English

LOAD-DATE: July 25, 2000

Doc #34

ABC NEWS
SHOW: WORLD NEWS TONIGHT (6:30 PM ET)

July 24, 2000, Monday

TYPE: Newscast
LENGTH: 442 words
HEADLINE: PRESIDENT CLINTON RETURNS TO CAMP DAVID TO ASSIST IN PEACE TALKS; BI DEFENDS E-MAIL MONITORING SYSTEM
ANCHORS: PETER JENNINGS
REPORTERS: JOHN COCHRAN
BODY:

PETER JENNINGS, anchor:

At Camp David in Maryland, day 14. The Israeli and Palestinian leaders have been holed up for two weeks now with hardly a leak to the news media, which in itself is quite remarkable. President Clinton, just back from Japan, spent much of last night and most of today in the talks, desperately, we are told, trying to coax the parties into some kind of a deal. ABC's John Cochran is covering Camp David for us.

John, looking at your notes today, 'Not looking good, senior administration officials will take a miracle,' say the Palestinians, doesn't look good at all?

JOHN COCHRAN reporting:

That's right, Peter. A senior administration official told me, just a short time ago he believes the talks will end one way or the other this week and he was not particularly optimistic. On top of that, Palestinian officials told ABC News, they believe it will take a miracle to achieve a breakthrough. The key stumbling block, not the only stumbling block, but the key one, continuing to be Jerusalem. So much so, that today, the negotiators simply took that subject off the table and concentrated on other issues.

JENNINGS: So why did they take--John, John, why do they take Jerusalem off the table and expect they can get anywhere like a deal?

COCHRAN: Well, what they would like to do is to try to get an agreement on land and security and they are getting the director of the CIA, George Tenet, to help them on this security issue. If they can resolve those issues, maybe they can go back to--to the issue of Jerusalem. What they would like, Peter, is to get at least a partial agreement this week, something that will enable both sides to come back at least in August and keep banging away.

JENNINGS: OK, John Cochran covering Camp Maryland for us. There's the key phrase, partial deal. Jerusalem has always, always been the final issue.

The FBI was on Capitol Hill today defending its e-mail monitoring system, the ominous-sounding Carnivore, against concerns that it casts too wide a net. The agency told Congress today it only uses the system to eavesdrop on suspected terrorists, computer hackers and other criminals, not on law-abiding citizens. Some people will not be convinced.

When we come back, a plague of grasshoppers in Texas.

Mr. JAMES ROBINSON (Entomologist): These are some of the worst outbreaks of insects for our cattlemen in the state that I've witnessed.

JENNINGS: And surviving a storm off the Louisiana coast. Was it murder or self-preservation?

Doc. #35

Announcer: WORLD NEWS TONIGHT with Peter Jennings and A CLOSER LOOK, brought to you by...

(Commercial break)

LANGUAGE: English

LOAD-DATE: July 25, 2000

SHOW: CBS EVENING NEWS (6:30 PM ET)
July 24, 2000, Monday

TYPE: Newscast
LENGTH: 462 words
HEADLINE: NEW SURVEILLANCE SOFTWARE ALLOWS THE FBI TO SNOOP THROUGH COMPUTER USERS' E-MAILS
ANCHORS: JOHN ROBERTS
REPORTERS: JIM STEWART
BODY:

JOHN ROBERTS, anchor:

Top officials of the FBI went to Capitol Hill today to respond to lawmakers' concerns about a sophisticated e-mail surveillance program and its potential for abuse. Critics fear this new software makes government snooping so easy, it leaves ordinary Americans vulnerable to invasion of privacy. CBS' Jim Stewart has more.

JIM STEWART reporting:

Every day, more than a billion e-mails are sent and received by computer users, and the FBI thinks criminals are now just as fond of them as the next guy. But the problem for agents has always been: Just how do you sort through all the gibberish to find any meaningful evidence? Today, the bureau told Congress it thinks it's found the answer in a software program called Carnivore.

Mr. LARRY PARKINSON (General Counsel, FBI): This is--despite its unfortunate name, this is a tool that is very surgical.

STEWART: Essentially, Carnivore is like a wiretap on the Web. Physically, it's nothing more than a small computer the FBI can lock inside the switching room of an Internet service provider like, say, America Online. But instead of reading every AOL customer's e-mail, it's designed to zero in and record just the messages sent to and from one particular e-mail address.

Mr. DONALD KERR (Director, Lab Division, FBI): We don't do broad searches or surveillance with this system. That's not authorized by a court order and, in my view, could not be.

STEWART: Critics, however, immediately asked: Who's watching the watchers?

Mr. ALAN DAVIDSON (Center for Democracy & Technology): Carnivore has access to much more information than it is legally entitled to collect. How do we know that we can trust Carnivore? How do we know what kind of leash has been put on Carnivore?

STEWART: The reason for the skepticism is because there's a big difference between wiretapping the Internet and wiretapping a telephone. If the FBI wants to bug your telephone, they get a court order and go to the phone company, and the phone company makes the connection for the bureau. If the FBI wants to wiretap your Internet address, they get a court order and then they can make the connection themselves.

They've done it 16 times this year already, mostly against Internet hackers, and the potential list of suspects and their crimes is growing, agents warned. Four years from now, the number of commercial e-mail messages alone is expected to top 200 billion a year. Jim Stewart, CBS News, Washington.

ROBERTS: And next up on the CBS EVENING NEWS, a new scheme to bilk the old

Doc. #36

and steal their trust.

(Graphic on screen)

CBS MarketWatch

DOW JONES INDUSTRIALS

CLOSE down 48.44 10,685.12

NASDAQ

CLOSE down 112.88 3,981.57

CBS.MARKETWATCH.COM

(Announcements)

LANGUAGE: English

LOAD-DATE: July 25, 2000

CBS News Transcripts

SHOW: THE OSGOOD FILE (Various Times)

July 25, 2000, Tuesday

TYPE: Commentary
LENGTH: 445 words
HEADLINE: FBI UNDER FIRE FOR USING INTERNET SOFTWARE TO WATCH SUSPECTS' E-MAILS
REPORTERS: CHARLES OSGOOD
BODY:
CHARLES OSGOOD reporting:

THE OSGOOD FILE. Charles Osgood on the CBS Radio Network.

The FBI is able to read supposedly private e-mail and other Internet traffic using a system called Carnivore. Carnivore, according to the dictionary, is any flesh-eating animal or plant. Not to worry, says the FBI.

Mr. LARRY PARKINSON (General Counsel, FBI): Despite its unfortunate name, this is a tool that is very surgical.

OSGOOD: Where have we heard that before? Stand by.

(Announcements)

OSGOOD: The American Civil Liberties Union is concerned, to say the least, about the FBI's Carnivore system for snooping on the Internet.

Unidentified Man #1: This is the equivalent of going to the post office and stationing an FBI agent there looking at the addressing information of every letter that goes through.

OSGOOD: No, it's nothing like that at all, says the FBI Lab Division's Donald Kerr.

Mr. DONALD KERR (FBI Lab Division): We don't do broad searches or surveillance with this system.

OSGOOD: 'The bureau is being very scrupulous about not violating anybody's civil rights with Carnivore,' says the FBI general counsel Larry Parkinson.

Mr. PARKINSON: This is a tool that is deployed rarely and it is never deployed without a court order.

OSGOOD: In other words, 'Trust us.' 'Not good enough,' says Alan Davidson of the Center for Democracy and Technology.

Mr. ALAN DAVIDSON (Center for Democracy and Technology): Carnivore has access to much more information than it is legally entitled to collect. How do we know that we can trust Carnivore? How do we know what kind of leash has been put on Carnivore?

OSGOOD: The Justice Department says law enforcement officials have to follow crime wherever it leads. Deputy attorney general Kevin DiGregory.

Mr. KEVIN DiGREGORY (Deputy Attorney General): Many of the crimes that we confront every day in the physical world are beginning to appear in the online world.

OSGOOD: For many of the abuses that occur in the physical world occur in the online world, too. That's why Congress is now taking an interest in

Doc. #37